サイバーセキュリティ通信【第15号】

平成30年2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

インターネットバンキング不正送金被害発生！！

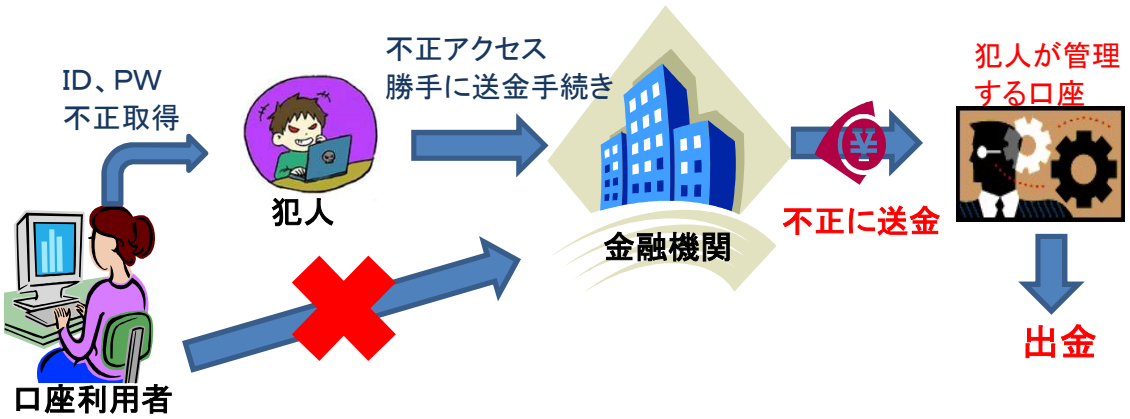
1 県内でインターネットバンキング不正送金被害発生!!

今月（平成30年2月）、県内の金融機関が提供するインターネットバンキングで、不正送金被害が発生しました。

手口も巧妙化しており、標的型メールによる**ウイルス**の感染や偽のサイトからパスワード等の入力を要求する場合（**フィッシング**）もあります。

今後も続発するおそれがあるため、注意をして下さい。

また、ビットコインなどの**仮想通貨**に対する不正送金被害も全国各地で発生していますので、利用される方は十分に注意して下さい。



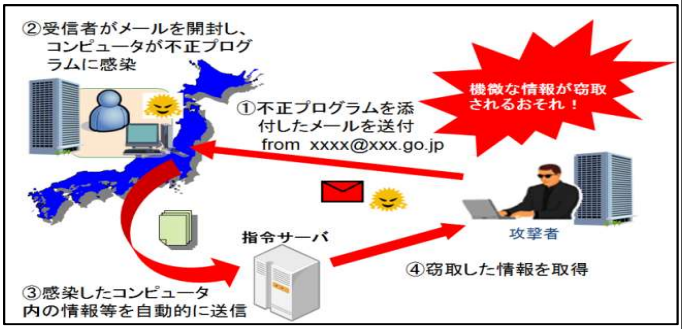
2 フィッシングと標的型メール

（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、知らず知らずに打ち込んだ住所、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が詐取される被害のことをいいます。

（2）標的型メールによるウイルス感染

標的型メールとは、サイバー攻撃のひとつで、業務に関連した正当なものであるかのように装いつつ、**不正プログラムを添付した電子メール**を送信し、これを受信したコンピュータを不正プログラムに感染させることによって、個人情報を流出させたり、インターネットバンキングの不正送金やランサムウェアなどに感染させてデータが暗号化されるなどの被害に遭うおそれもあります。



３　セキュリティ対策について

①　パソコンのOS、ソフトウェアを最新の状態にする

標的型メールに添付されている不正プログラムは、パソコンのOSやインストールされている各ソフトのぜい弱な部分を狙って侵入します。

OSやソフトウェアは、常に最新の状態に更新しましょう。

②　ウイルス対策ソフトを導入し、最新の状態に更新する

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う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　心当たりのないメールを安易に開かないこと

心当たりのないメールに添付されたファイル（特にexeファイル、ZIPファイル）がウイルスであったり、リンク先がフィッシングサイトである可能性があります。

安易に開いたり、本文に記載のURLに不用意にアクセスをしないで下さい。

④　ワンタイムパスワード等金融機関のセキュリティ対策を積極的に利用

不正送金被害を防止するためには、携帯電話のメールアドレスやトークン（ワンタイムパスワード生成器）を使ったワンタイムパスワードの利用が効果的です。

実際、ワンタイムパスワードを設定していたことにより、被害防止につながった事例がたくさんあります。

金融機関が提供するセキュリティ対策もあるので、詳しくは口座を開設している金融機関に相談して、積極的に利用しましょう。

⑤　慌てず落ち着いた対応

そもそも、正規なメールには、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の内容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。

⑥　組織対応と情報共有

企業や団体であれば、セキュリティポリシーを定め、従業員には日頃からセキュリティの意識を高めるための教育、指導が必要です。

また、不審なメールを受け取った場合には、メールの情報・内容をいち速く共有することで、被害の拡大を防止することが出来ます。

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