

フィッシング詐欺誘引メール！

フィッシング詐欺の手口と、その対策！



迷惑メールの手口は、日々、複雑巧妙になっています。ここ数年問題になっているのが「フィッシング詐欺」です。フィッシング詐欺とは、銀行やクレジットカード会社を装い偽メールを送り付け、その文中リンクから受信者を本物そっくりの偽サイトに誘導し、銀行口座や暗証番号、クレジットカード番号やID、パスワード等を入力させ、不正に個人情報を入手しようとする行為をいいます。

銀行からのメールを装った偽メール

本物そっくりの偽銀行サイト

From : aaa@x x x . jp
Sub : ○○銀行からお客様へ
緊急のお知らせ

セキュリティのため、ID と
パスワードの再登録手続き
を、下記のページよりして
下さい。

[http://www.x x ~○○~
x . com/tourouku/](http://www.x x ~○○~
x . com/tourouku/)

○○銀行再登録ページ

ユーザ - ID

1028abcxyz002085

パスワード

口座番号 0670578

**ID やパスワード、
口座番号等、重要な
情報が悪徳業者に悪
用される**



フィッシング詐欺の被害

- ・クレジットカード情報の不正利用
- ・銀行預金の不正出金
- ・インターネットオークションにお
けるなりすまし
- ・個人情報の不正売買

クリックすると

登録

登録してしまうと

ポイント

1 最近のフィッシング詐欺

最近のフィッシング詐欺は、偽の Web サイトも本物の Web サイトと区別がつかないようにするなど、手口が巧妙化しており、ひと目ではフィッシング詐欺と区別がつかないケースも増えています。

2 フィッシング詐欺対策

- ① **メールに書かれているURLをむやみにクリックしない。**
あやしいと感じる電子メールには返信しない。また、書かれているURLにもアクセスしないことが大切です。
- ② **個人情報やID、パスワード等を、むやみに入力しない。**
フィッシング詐欺の目的は、暗証番号や口座番号、クレジットカード番号等、個人の重要な情報を手に入れることです。自分の利用している銀行やクレジット会社からの電子メールであっても、個人情報やID、パスワードは不用意に入力しないで下さい。
- ③ **メールの内容をそのまま信用せず、名前を使われた機関の窓口にお問い合わせ、確認する。**
個人の重要な情報を尋ねる電子メールが届いた場合は、名前を使われた機関へ必ず電話等で問い合わせ、内容について裏付けを取ることが重要です。
信頼できる会社は、電子メールで個人の重要な情報を聞いてくることはありません。

3 もしもトラブルに遭遇してしまったら

個人情報を入力した後で、フィッシング詐欺に遭ったことに気が付いた時は、すぐに保護者に相談するとともに、実際の銀行やクレジット会社に連絡をして、口座やカードの利用を止めて下さい。

被害に遭った場合には、すぐに最寄りの警察署か都道府県警察本部のサイバー犯罪相談窓口（フィッシング110番）に相談して下さい。

フィッシング詐欺誘引メール

<事例>

● ハンゲームの偽ホームページを使ったフィッシング詐欺（2006年5月30日）

オンラインゲーム（ハンゲーム）の偽ホームページを作り、個人情報を盗む「フィッシング行為」をしたとして、名古屋市内の中学3年の男子生徒（14歳）が、[不正アクセス禁止法](#)違反と著作権法違反の容疑で書類送検された。未成年者がフィッシング行為で摘発されるのは全国で初めて。少年は盗み取った小中学校の少女のIDやパスワード等を勝手に変更し、「ホームページに入れるようにしてほしいから裸の写真を送れ」と脅迫メールを送り、数十人からわいせつな写真を送らせていた。

● UFJ銀行をかたるフィッシング詐欺メール（2005年3月15日）

UFJ銀行の名前をかたってパスワード等を盗み取ろうとする、フィッシングメールが出回った。「セキュリティの向上に伴いまして、オンライン上でのご本人確認が必要となります。この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします」とメールが届き、メールに書かれたアドレスで偽の銀行ホームページに接続。カード番号や暗証番号等を入力させ、その情報を使ってクレジットカードを偽造、現金引き出しが行われた。同社は「当社から暗証番号の入力を求めるメールを送ることはない」と詐欺への注意を呼びかけた。

● Yahoo! JAPANをかたるフィッシング詐欺メール（2005年10月28日）

Yahoo!オークションの名前をかたったフィッシング詐欺メールが出回った。「Yahoo!オークションより重要なお知らせ。セキュリティチェックのため」等と称してメールが届き、メールに書かれたアドレスで偽のYahoo!オークションのホームページに誘導。Yahoo! JAPAN ID、パスワード、暗証番号等の個人情報をだまし取ろうとした。

そのほかにも、Yahoo! JAPAN の名前をかたって「あなたのパスワードが解読されたので指定のパスワードに変更して下さい」とメールが届き、パスワードを変更すると悪用されるケースもある。

● NTTドコモをかたるフィッシング詐欺メール（2008年2月1日）

NTTドコモやドコモのインフォメーションセンターになりすまして、「連絡がない場合には利用停止等を行う」といった内容のメールを送った上で、偽のNTTドコモのホームページに誘導し、利用者の個人情報を不正に聞き出す行為が発生した。NTTドコモでは、「お客様のプライバシー情報をメール等でお尋ねすることはありません」と注意を呼びかけた。

<用語解説>

● 不正アクセス禁止法（平成12年2月13日施行）

他人のIDやパスワードを無断で使って、ホームページ等にアクセスすることを犯罪として罰する法律。たとえば、オンラインゲーム等で勝手に他人のIDやパスワードを利用した場合は、この法律に違反します。ゲームのアイテムほしさに他人のIDを勝手に使って、ゲームサイトにアクセスした中学生や高校生がこの法律に違反したとして、検挙されたことがあります。（文部科学省 「ちょっと待って、ケータイ」より）

<関係機関の情報>

● 警察庁では全国の都道府県警察本部において、フィッシング詐欺の情報を集める「フィッシング110番」を開設しています。

（警察庁 フィッシング110番）

<http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>

（山口県警察 フィッシング110番）

<http://www.police.pref.yamaguchi.jp/O210/hitec/hitec12.htm>

● フィッシング対策協議会「STOP!フィッシング詐欺」 <http://www.antiphishing.jp/home.html>