Yahoo! JAPAN におけるフィッシング対策

2010年 1月 28日

R&D統括本部 セキュリティプラットフォーム技術

Project ZERO

ご挨拶

R＆D統括本部　セキュリティプラットフォーム技術

戸田 薫

Project ZERO

～全ての不正行為をゼロに～

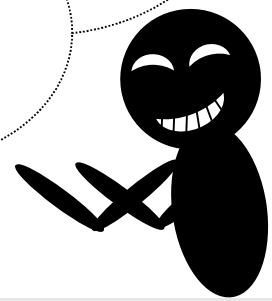
アジェンダ

1. フィッシングを仕掛ける動機とは？
2. 過去から現在までのフィッシングの変遷
3. その手口と傾向
4. Yahoo! JAPAN の取り組み
5. 今後の見通し

1. フィッシングを仕掛ける動機とは？

フィッシングを仕掛ける心理

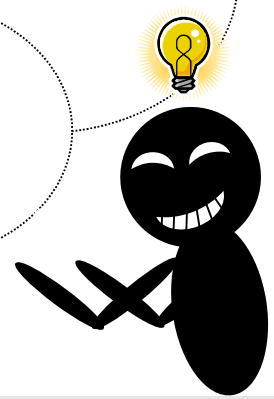
- 悪い事をしてでも儲けたい
- ネットならではの手軽さ
- 24時間いつでもどこでも
- 数打てば当たる
- 逃げるのが簡単
- 捕まっても軽い罪



Yahoo! JAPAN は格好のターゲット

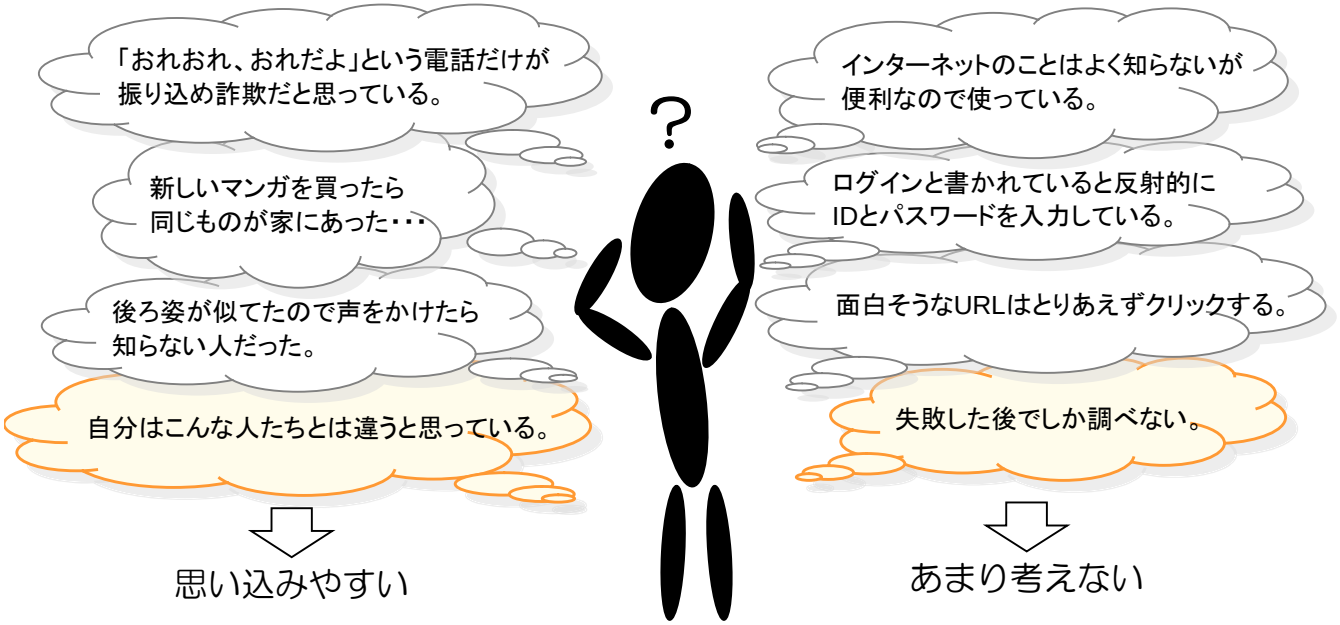
Yahoo! JAPAN ならユーザー多いし、
色々あるから狙ってみるか！

ユーザー数・サービス数の多さ、マネタイズの容易さがターゲット理由になってしまう・・・



こんな人はフィッシングに要注意

どんな人でも被害に遭う可能性があります。



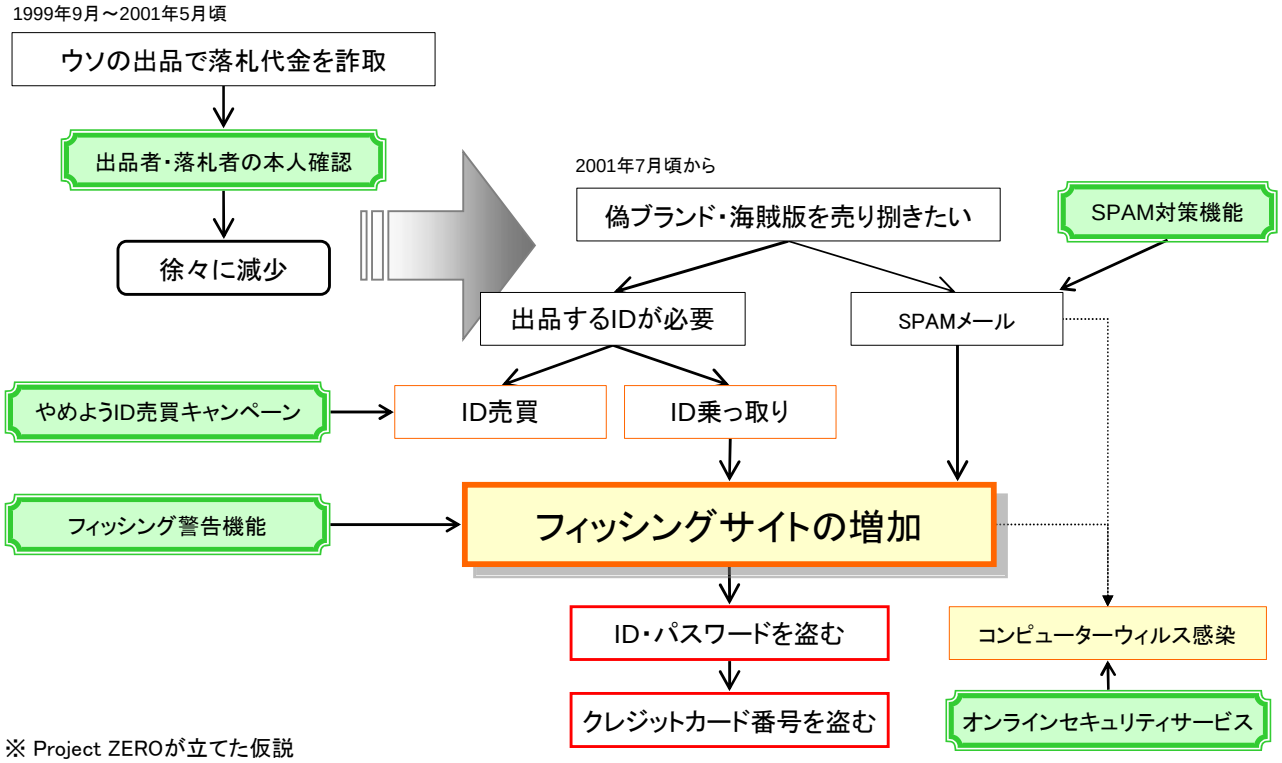
※ あくまでイメージです。

2. 過去から現在までのフィッシングの変遷

（画面をご覧ください）

このページは画面のみのご提供となります。

依然としてYahoo!オークションを騙るケースが多い



※ Project ZEROが立てた仮説

3. その手口と傾向

Yahoo! JAPANを装ったメール

効果的タイミングを狙い、信憑性を高める工夫をこらす

件名:【重要なお知らせです】

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

Date: Thu 28 Jan 2010 14:52:59 +0900 (JST)
From: ◆◆◆◆@yahoo.co.jp アドレスブックに追加
DomainKeys は、このメールが yahoo.co.jp から送信された
Subject:【重要なお知らせです】
To: ●●●●@yahoo.co.jp

Yahoo! Auctionsよりご案内です

いつもYahoo! Auctionをご利用頂きありがとうございます。
http://□□□□. □□□□. □□□□/yahoo-actions.co.jp
よりお客様の会員情報の更新をお願いします。
更新を行われない場合出品制限等の不具合を起こす場合
ありますのでご協力お願い致します。

※こちらのメールは自動送信メールとなっておりますので、そのままご返信いただき
ましてもお答えいたしかねます。

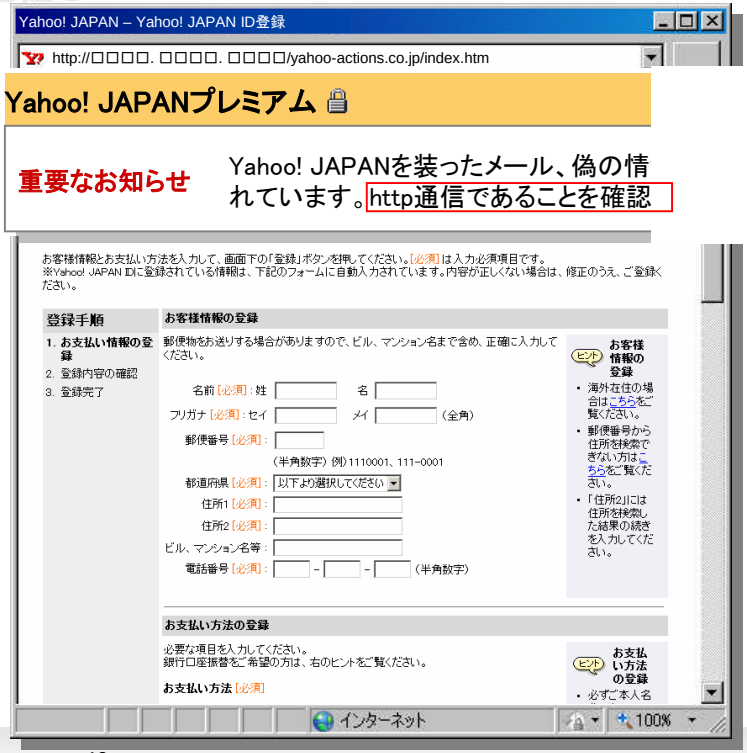
なになに、ヤフオクからのご案内？！
「会員情報の更新をお願いします」って
更新しないと出品制限されちゃうのか・・・

安全対策研究所・助手くん

セキュリティ対策は万全に

ブラウザの脆弱性が狙われる可能性も・・・

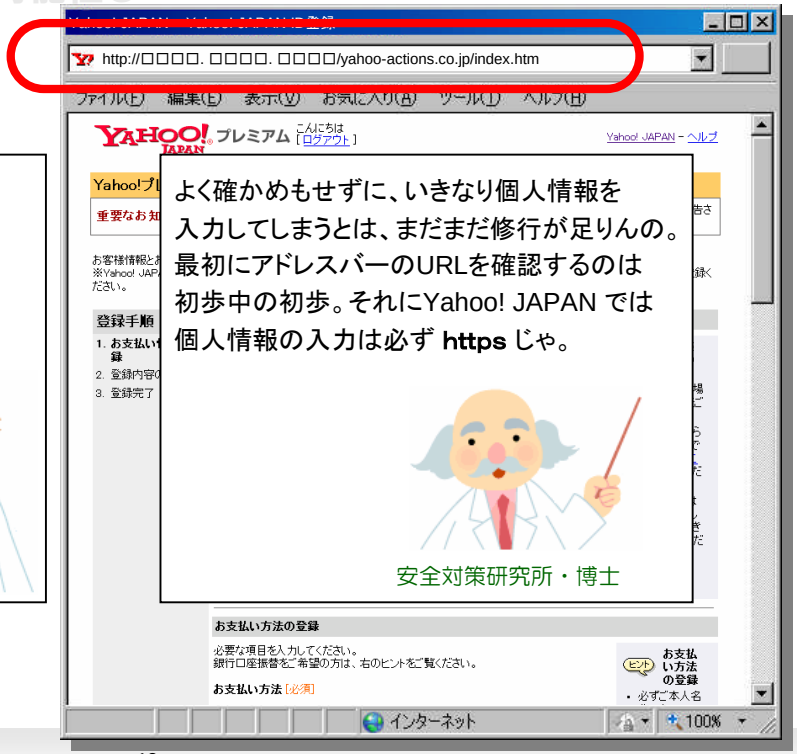
氏名と住所とクレジット番号っと・・・
これでいいのかな。それからえーっと、
「**http** 通信であることを確認」って何？！



セキュリティ対策は万全に

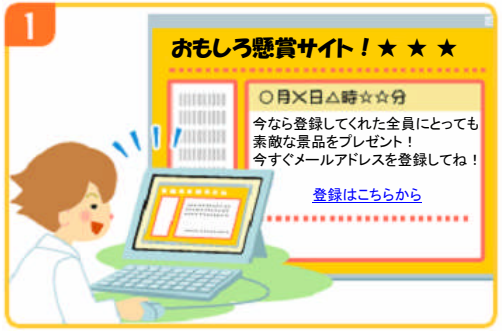
ブラウザの脆弱性が狙われる可能性も・・・

氏名と住所とクレジット番号っと・・・
これでいいのかな。それからえーっと、
「**http** 通信であることを確認」って何？！



外部で盗んでYahoo! JAPANで悪用する

1. 「A」という懸賞サイトにYahoo! JAPANと同じパスワードとYahoo! メールのメールアドレスを登録した。



2. 実はその懸賞サイト「A」は犯罪者が運営するサイトだった！

3. 犯罪者は、Yahoo!メールアドレスの@より前の文字列（Yahoo! JAPAN IDと同じ文字列）と、懸賞サイトに登録されたパスワードでYahoo! JAPANにログインを試した。

4. Yahoo! JAPAN IDのパスワードと懸賞サイトに登録されたパスワードが同一 のためログインに成功し、Yahoo! JAPAN IDを不正利用してオークションに出品されてしまった。

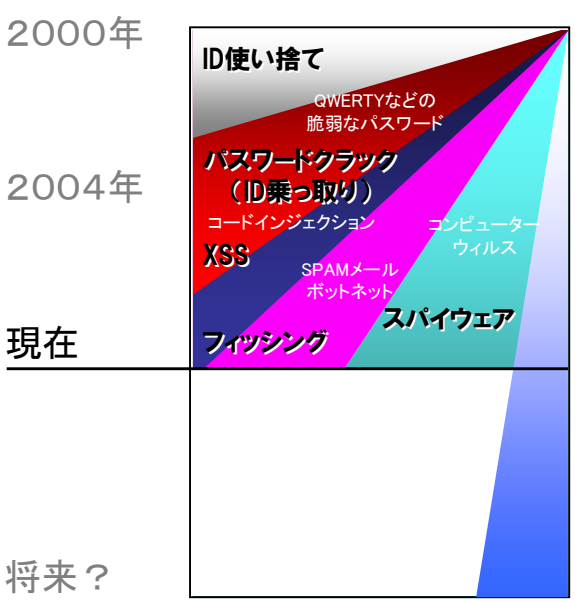
日本国内のフィッシング詐欺グループ逮捕

犯人グループの手口

1. 大量のメールアドレスを入手してフィッシングメールを送信
2. フィッシングサイトに誘導してクレジットカード番号を盗み出す
3. 盗み出したクレジット番号でショッピングサイトから家電製品を購入
4. 私設の私書箱に商品を送らせ秋葉原などで転売

複雑化するコンピューターセキュリティへの脅威

セキュリティの仕事を通して見えてきた手口の移り変わりとは・・・



未知のセキュリティ脅威？

単純な手口を試行錯誤

▽

サービス提供側を攻撃

▽

利用者側の脆弱性を攻撃

▽

油断していると誰もが被害にあう時代

４. Yahoo! JAPAN の取り組み

Yahoo! JAPANのログインページ

ログインページには様々な機能があります。

重要なお知らせ さらに使いやすく便利になった「**ログインアラート**」があなたのYahoo! JAPAN IDを守ります！いつでもどこでも不正ログインを検知できるようにケータイのメールアドレスを設定しよう！

Yahoo!ツールバーのフィッシング警告機能は、Yahoo! JAPANであるかのように装い、Yahoo！JAPAN IDやパスワードなどを不正に取得しようとするサイトを表示すると、警告画面を出して注意を促します。

PR

Yahoo! JAPANへ
ログインしてください

Yahoo! JAPAN ID:

パスワード:

☐ **次回からIDの入力を省略**
共用のパソコンではチェックを外してください。

ログイン

Yahoo! JAPAN IDを
お持ちでない方

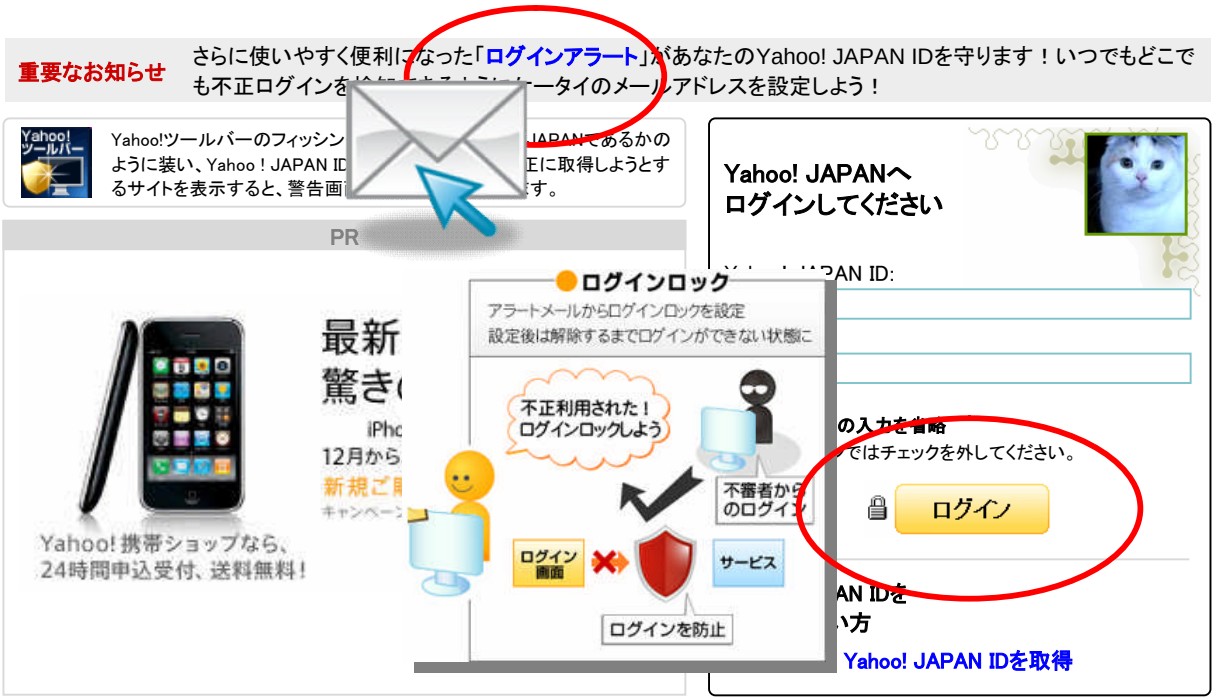
Yahoo! JAPAN IDを取得

ログインアラート：ログインをメール通知

認証されたメールアドレスへログインされたことを通知します。

ログインロック：不審者のログイン試行をブロック

ログインロックは利用者で解除することができます。

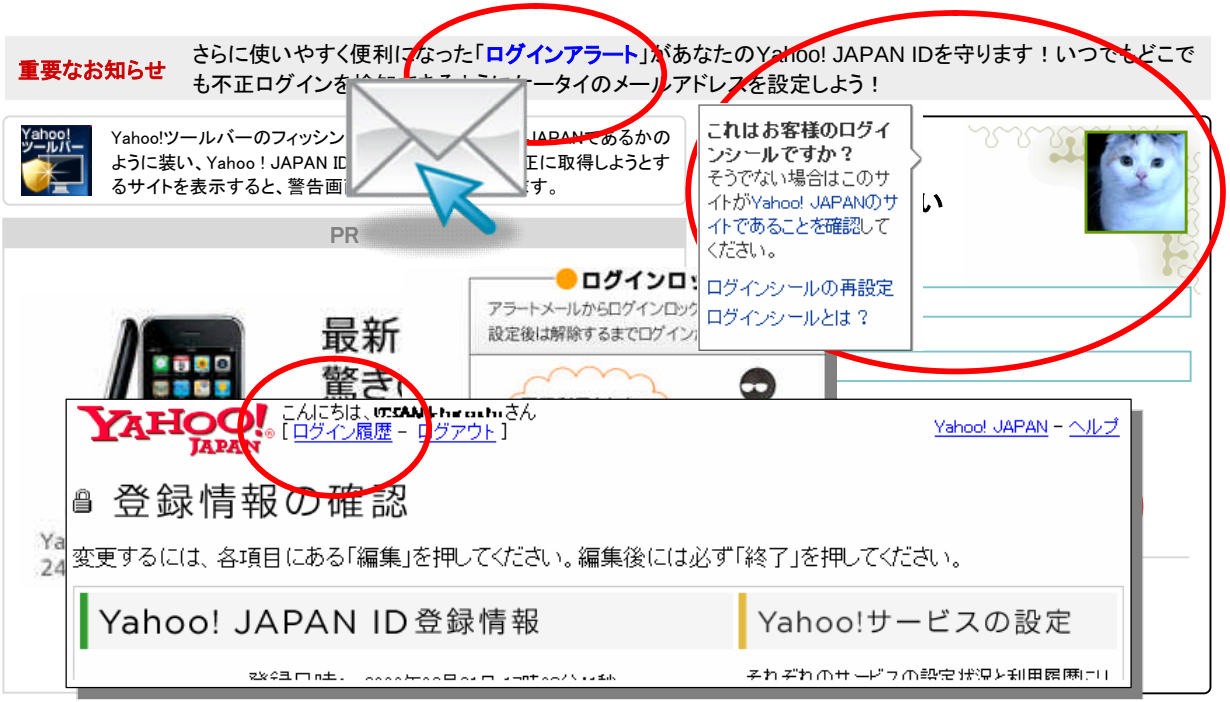


ログインシール：自分だけの画像が目印

普段使っているパソコンに自分だけの画像を設定できます。

ログイン履歴

登録情報ページからログイン履歴を見ることができます。



ログイン履歴：不審なログインの発見手段

身に覚えの無い日時・IPアドレスなどをチェックできます。

こんにちは●●●●さん
[ログアウト]

Yahoo! JAPAN － ヘルプ

●●●●さんのログイン履歴

最終更新日時：2010年01月28日（木曜日）17時06分

サービスへ戻る

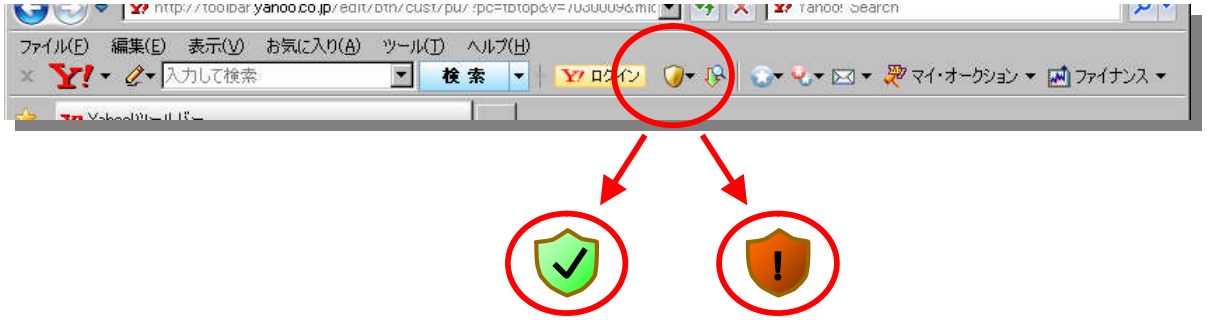
ログイン履歴ページは、お客様が最近Yahoo! JAPANにログインを試みた履歴を、過去60件分表示しています。
詳細はヘルプをご覧ください。認証形式、IPアドレスなど各項目の意味については「ログイン履歴ページの見方」をご覧ください。

60件中1～30件を表示しています。　［前の30件｜次の30件］

Yahoo! JAPAN ID / ニックネーム	日時	サービス	認証形式	認証結果	IPアドレス	端末情報
●●●●	2010年01月28日（木）17時06分53秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月28日（木）17時06分45秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月28日（木）16時56分52秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月28日（木）16時56分36秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月28日（木）10時07分54秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月27日（水）13時38分24秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月27日（水）11時23分03秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月26日（火）08時44分54秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月22日（金）13時39分33秒	トップページ	ログイン	成功	192.168.8.248	パソコン

Yahoo!ツールバー ver.7.3：フィッシング警告機能

Yahoo!ツールバー ver.7.3以降でフィッシング警告機能が強化されました。



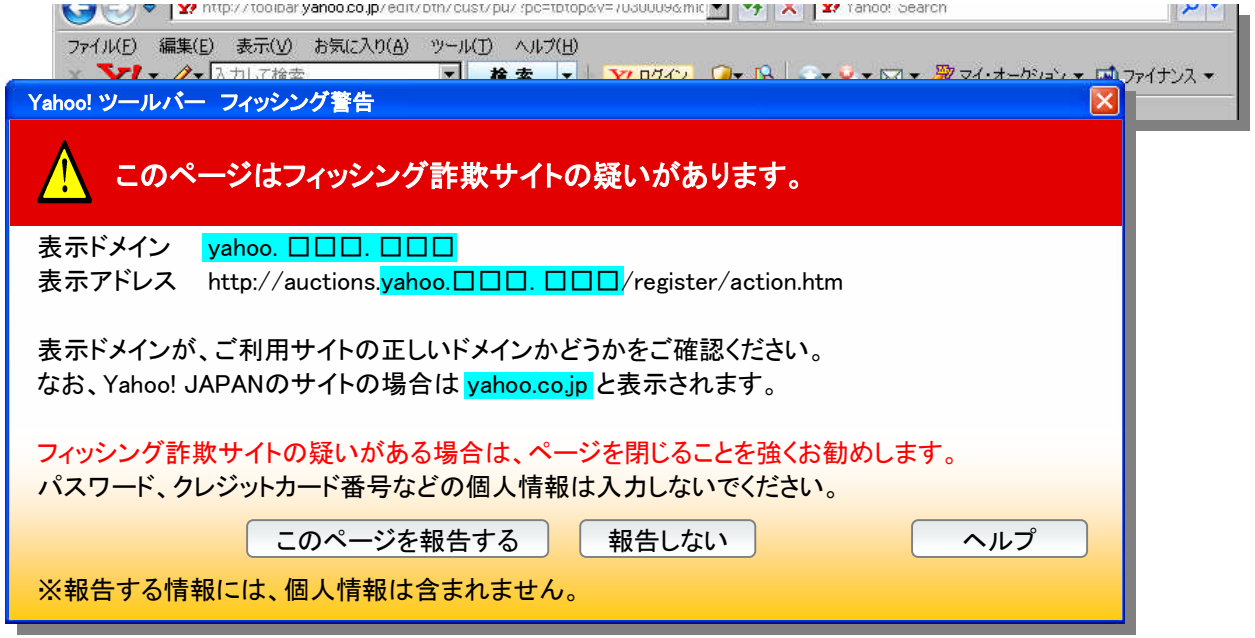
SSLで保護されたYahoo! JAPANのページを表示したときは緑色に変わります。

個人情報の入力に注意が必要なときは、ボタンの色がオレンジに変わってお知らせします。

Windows版 Yahoo!ツールバーVer.7.3以降

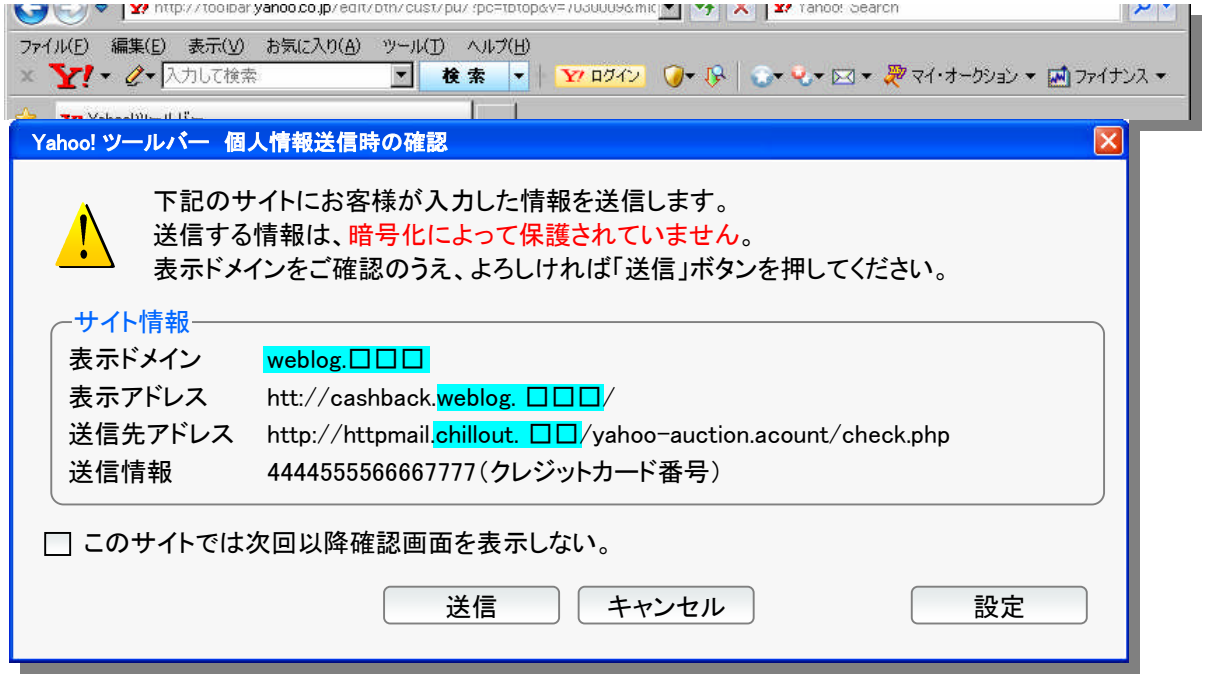
Yahoo!ツールバー：フィッシングサイトを警告

Yahoo!あんしんねっと からフィッシングサイト情報を取得してお知らせします。



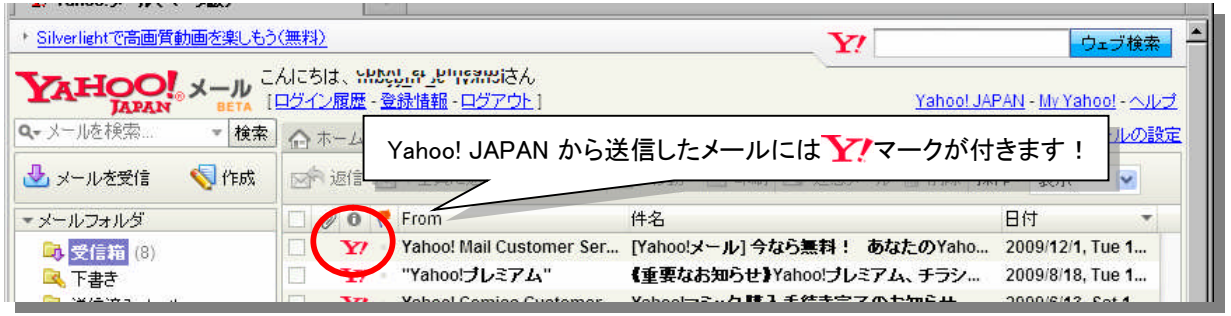
Yahoo!ツールバー ver.7.3：個人情報の送信を確認

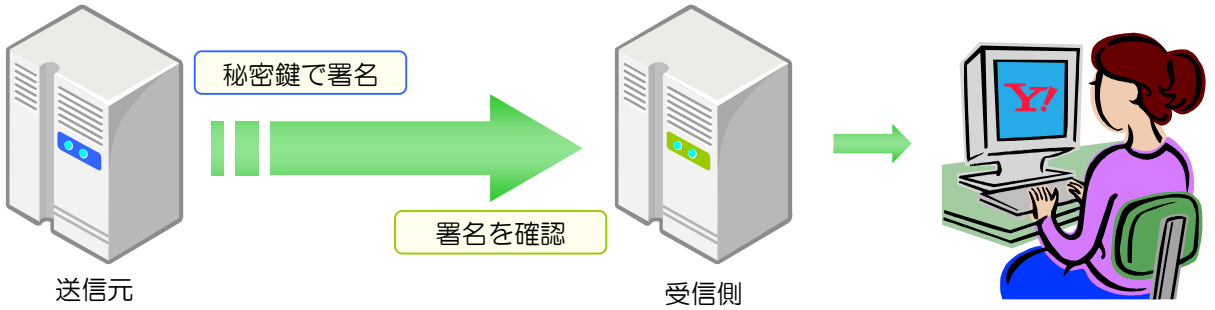
クレジットカード番号などの重要情報送信を判定してお知らせします。



Yahoo!メールのフィッシング対策機能

Yahoo!メールを使うと、Yahoo! JAPANからのお知らせが一目で分かります。





啓蒙活動への取り組み

多くの人が訪れるYahoo! JAPANだからできる取り組み

やめようID売買（啓蒙活動のご紹介）

Yahoo! JAPANでは、Yahoo! JAPAN IDの第三者への譲渡、貸与などを禁止しておりますが、残念ながら売買されるケースが確認されています。売買されたYahoo! JAPAN IDは、詐欺などの不正行為を行う第三者に渡り、悪用されていますので絶対にやめましょう。

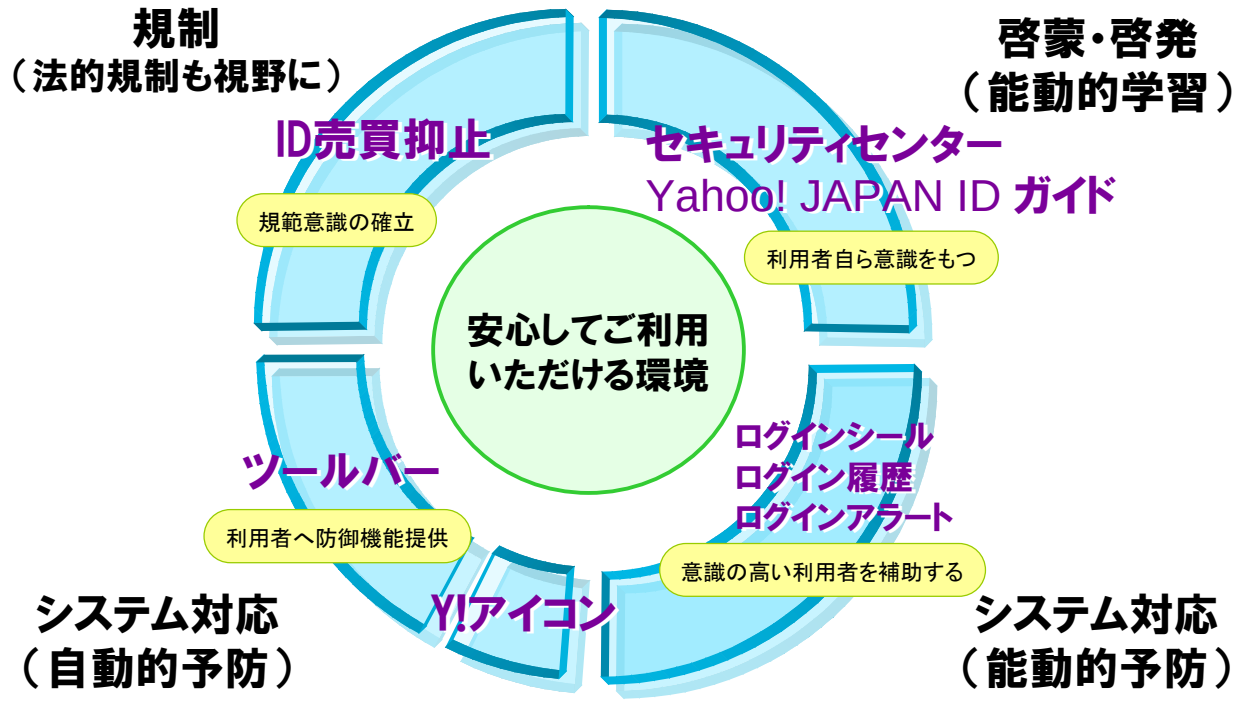
権利譲渡および商用目的使用の禁止（Yahoo!オークション ガイドラインより）

利用者は、このガイドラインの定めに従って取得した権利義務およびYahoo! JAPAN IDを第三者に譲渡、貸与等してはならないものとします。また利用者はYahoo!オークションをYahoo! JAPANのガイドラインで定める使用範囲、使用方法を超えて、Yahoo! JAPANの許可なく商用の目的で使用してはならないものとします。

みなさんにお願いしたいこと

Yahoo! JAPAN IDの第三者への譲渡、貸与等は有償、無償を問わず一切行わないでください。また、売買を持ちかけるメールやウェブサイトなどを発見した場合には Yahoo!オークションまでご報告ください。皆さまのご協力が安全なYahoo!オークションの礎になります。

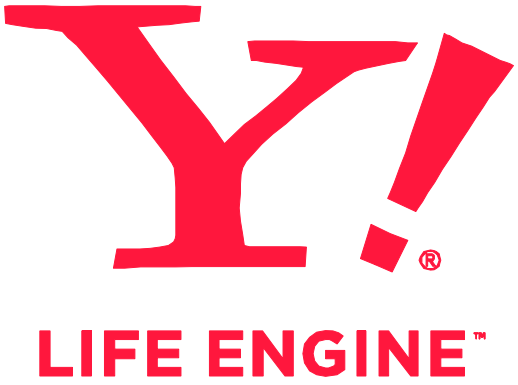
安心して利用できるインターネット環境へ



５. 今後の見通し

（画面をご覧ください）

このページは画面のみのご提供となります。



ありがとうございました。