# マルウェアとID盗難

フィッシング対策協議会技術・制度WG副主査
ウェブルート・ソフトウェア株式会社
野々下 幸治

Webroot Software, Inc.

# 目次

Privacy. Protection. Peace of mind.

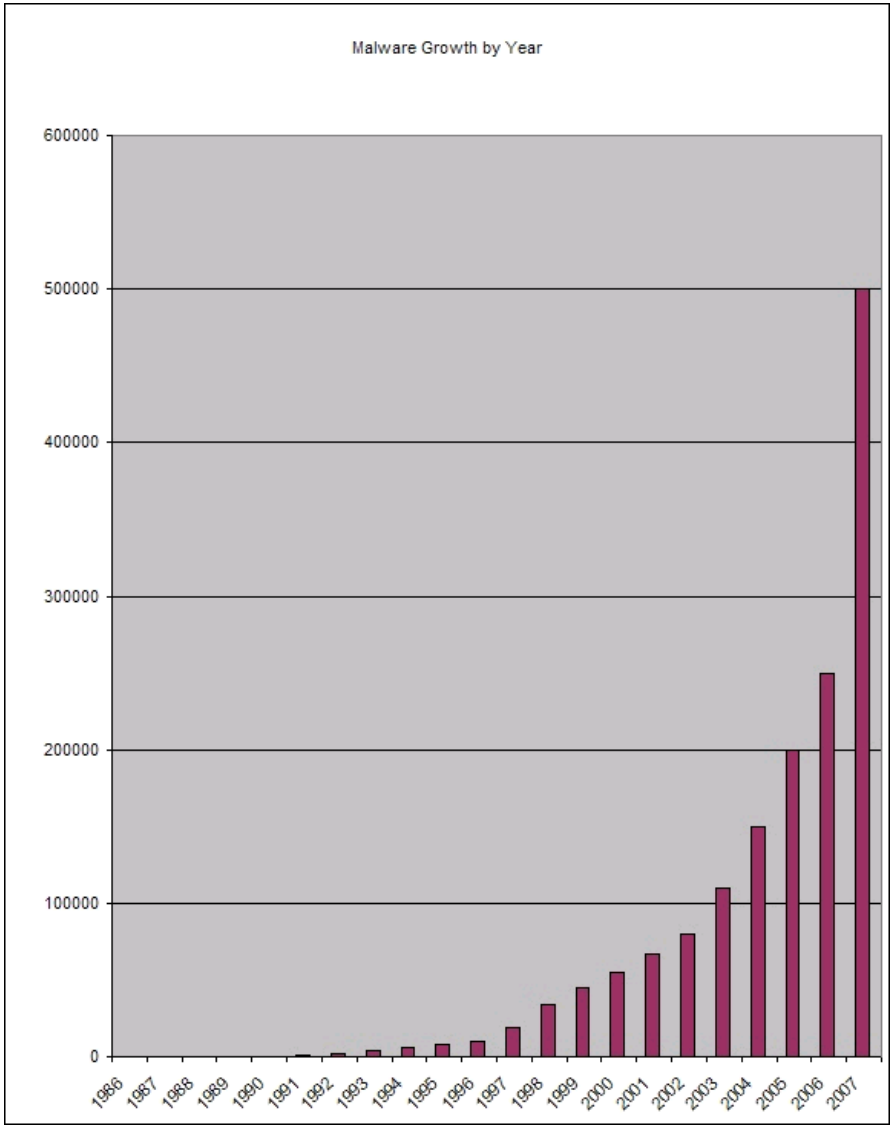
- 最近のマルウェアの状況
- ID盗難の現状
- 従来の常識が通用しないマルウェアの現状
- 対策
- フィッシング対策協議会の役割

# 最近のマルウェアの現状

Webroot Software, Inc.

# 指数関数的に伸びるマルウェアの数

Privacy. Protection. Peace of mind.

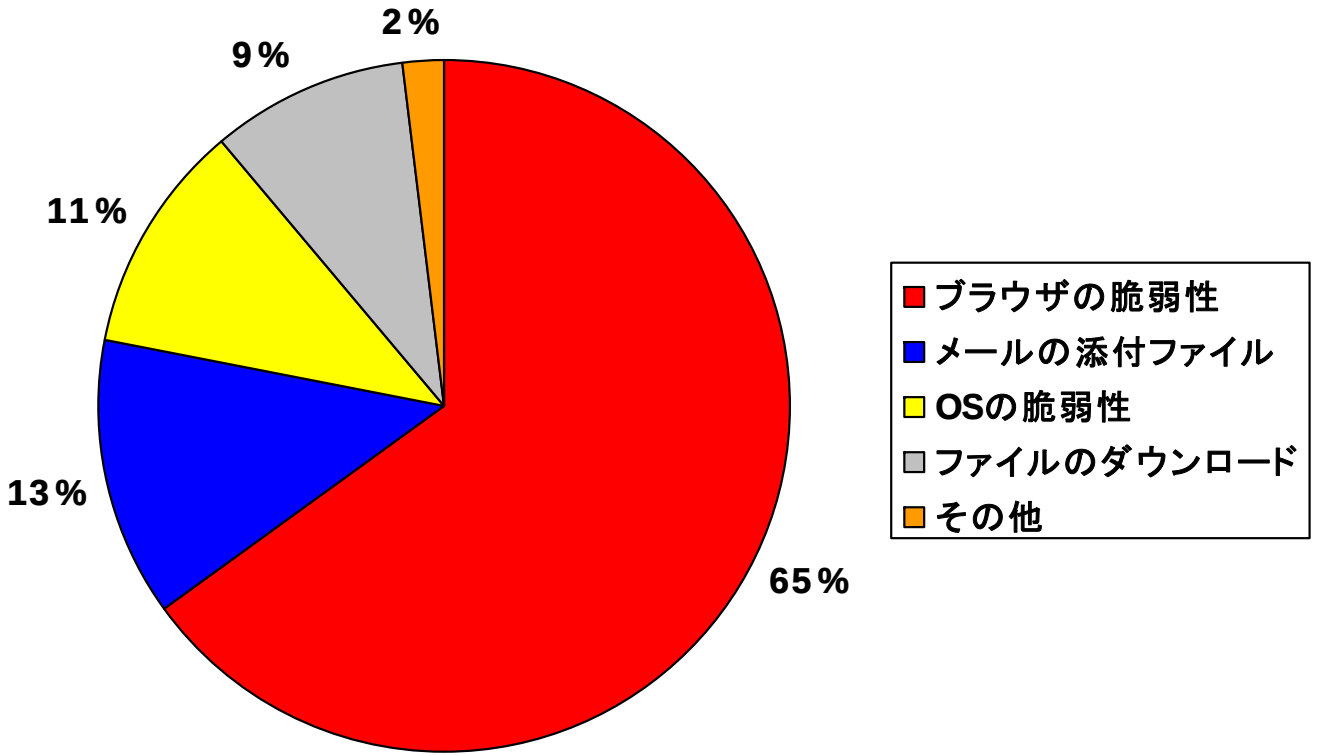


Webroot Software, Inc.

# マルウェアの感染経路

Privacy. Protection. Peace of mind.

- 半数以上がブラウザの脆弱性により感染
- 従来OSの脆弱性による感染を広げていたBotもブラウザの脆弱性からに変更




S21sec 2007年調査

Webroot Software, Inc.

# 亜種の出現ランク

Privacy. Protection. Peace of mind.

FIGURE 32. Number of variants per family

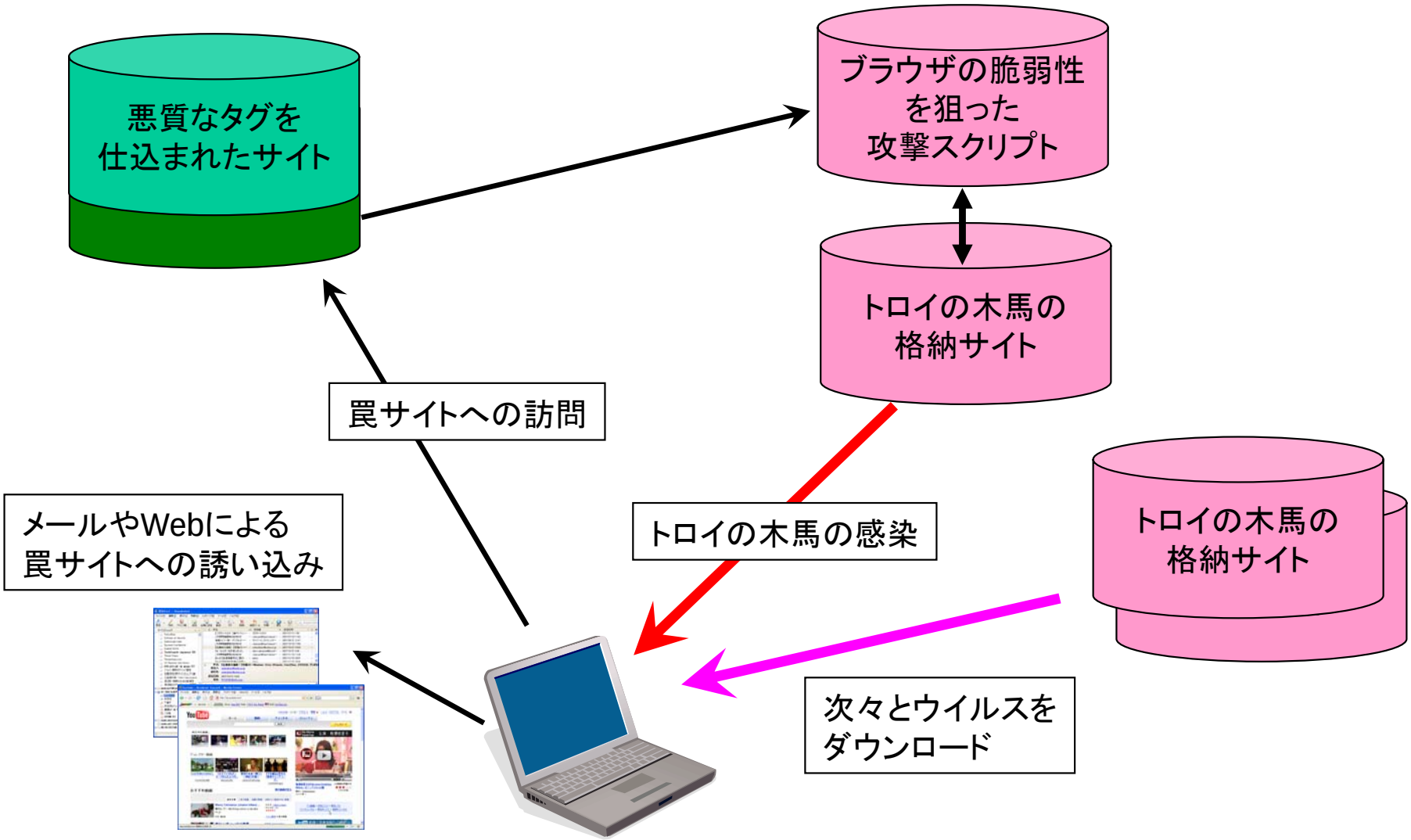
| 1H07 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rank | Malware Family | E-Mail | P2P | IM | Exploit | Back-door | Rootkit | Virus | PWS/ Key logger | Down-loader/ Dropper | Trojan | Number of variants (1H07) |
| 1 | HTML/IframeRef | | | | ● | | | | | | | 85,884 |
| 2 | Win32/Vxidl | | | | | | ● | | | ● | ● | 77,159 |
| 3 | Win32/Hupigon | | | | | ● | | | ● | ● | | 29,014 |
| 4 | Win32/Nuwar | ● | | | | | | | | | | 27,279 |
| 5 | Win32/Busky | | | | | | | | | ● | ● | 22,019 |
| 6 | Win32/Bagleziр | ● | | | | | | | | | | 20,461 |
| 7 | Win32/Zlob | | | | | | | | | ● | | 19,884 |
| 8 | Win32/Small | | | | | ● | | | | ● | ● | 14,240 |
| 9 | Win32/Horst | | | | | | | | | | ● | 12,801 |
| 10 | Win32/Scano | ● | | | | | | | | ● | | 12,338 |

マイクロソフト セキュリティ インテリジェンス レポート2007 年上半期の結果より

Webroot Software, Inc.

# 悪質なトロイの木馬に感染する仕組み

Privacy. Protection. Peace of mind.



Webroot Software, Inc.

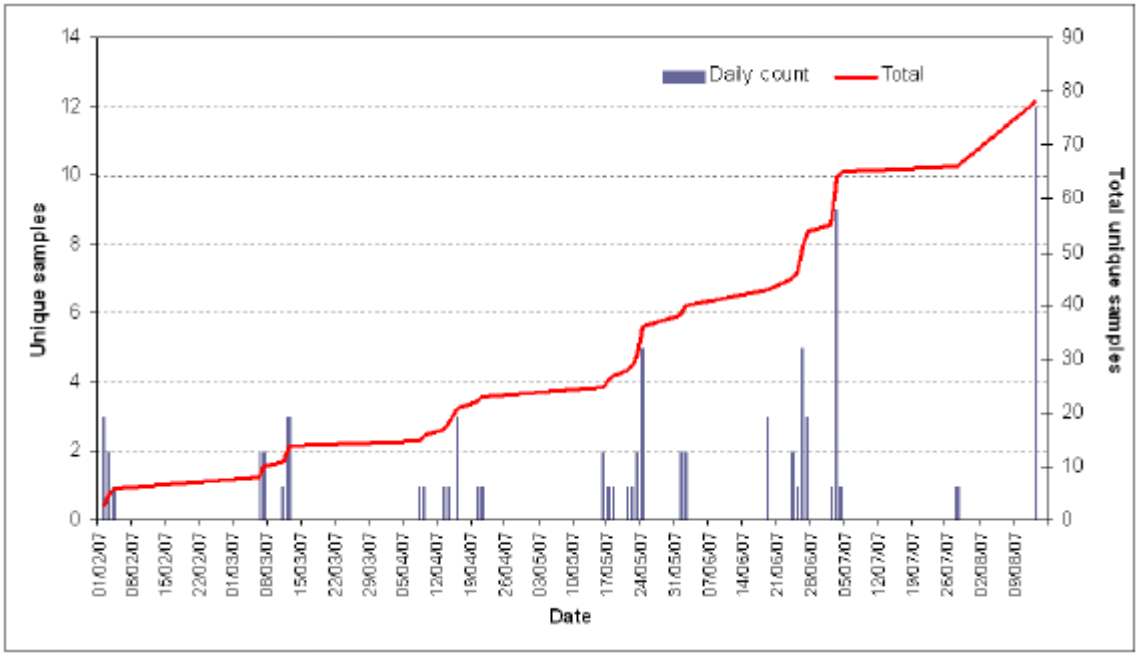
# トロイの木馬の頻繁な更新

Privacy. Protection. Peace of mind.

- 頻繁に更新を行いウイルス対策ソフトに検地されにくくする。

| ファミリー | 平均の更新日 |
|---|---|
| Mal/ObfJS | ＜1 |
| Mal/Dorf | 1 |
| Mal/Clagger | 1.5 |
| Mal/Dropper | 3 |
| Mal/DownLdr | 3.5 |
| Troj/Pushdo | 4 |

1ヶ月間での平均の更新率




2007年2月のClaggerのサンプルの一日の発見数
By Sophos

# ID盗難の実態

Webroot Software, Inc.

# Internet犯罪者の経済

Privacy. Protection. Peace of mind.

- 犠牲者からの直接的な経済的搾取
  - オンライン銀行からの預金の引き落とし
  - クレジットカードの利用
  - 脅しによる金銭請求
    - DDoS攻撃
    - ランサムウェア
  - 詐欺による搾取
- 犠牲者のアカウントを使っての間接的な経済的な搾取
  - PPCやPPIによるアフィリエイトの利益の取得
    - アドウェアのインストール
    - ボットによる広告のクリック
  - アカウントを利用したオークション詐欺による第三者からの取得
  - RMTによる利益
  - アカウントの第三者への販売
  - SPAM送信やDDoSマシンの販売

Webroot Software, Inc.

# オンラインアカウント

Privacy. Protection. Peace of mind.

- オンライン銀行
- ISPのアカウント情報
- 無料のメールアカウント
- Yahoo ID
- SNSのアカウント
- オンラインゲームアカウント

オンラインアカウントがいろいろな役割を広げつつある

犯罪者にとってはリスクが低くいIDでも、利用価値が上がっている

Webroot Software, Inc.

# 全銀協によるインターネット･バンキングの被害調査

Privacy. Protection. Peace of mind.

「インターネット･バンキングによる預金等不正引出し」に関するアンケート結果

（対象：正会員・準会員 182 行）

（単位：件、百万円）

| 時　　期 | 件　　数 | 金　　額 |
|---|---|---|
| 平成 17 年 4 月～6 月 | 2 | 1 |
| 平成 17 年 7 月～9 月 | 13 | 12 |
| 平成 17 年 10 月～12 月 | 16 | 13 |
| 平成 18 年 1 月～3 月 | 8 | 4 |
| 平成 18 年 4 月～6 月 | 4 | 12 |
| 平成 18 年 7 月～9 月 | 15 | 13 |
| 平成 18 年 10 月～12 月 | 17 | 14 |
| 平成 19 年 1 月～3 月 | 30 | 18 |
| 平成 19 年 4 月～6 月 | 41 | 58 |

Webroot Software, Inc.

# 警視庁ハイテク事件簿からのID盗難の事件 1

Privacy. Protection. Peace of mind.

- 19件中11件がID盗難に絡む事件、またそのうち2件が直接的な金銭被害

| 検挙年月日 | 事案 | 内容 | 適用罪名、罰条 |
|---|---|---|---|
| 平成19年3月28日 | ネット銀行に対する不正アクセス禁止法違反、私電磁的記録不正作出・同供用事件の被疑者の逮捕 | 被疑者は、ひったくりで得た他人名義のネット銀行口座のキャッシュカードやID、パスワードを用いて、携帯電話で同銀行の管理するサーバーコンピュータに不正アクセスし、利用停止手続きがされていた同口座を再開させるなどして、現金110万円を引き出していました。 | 不正アクセス禁止法違反<br>私電磁的記録不正作出・同供用罪 |
| 平成19年3月6日 | インターネット証券会社に対する不正アクセス禁止法違反被疑者の逮捕 | 被疑者は、インターネット証券会社のサーバーコンピュータ（委託会社が保守管理）に対し、自分で作成したプログラムを使い、他人のユーザIDを不正に入手した上、不正アクセス行為を行い、他人の取引状況などを勝手に閲覧しました。 | 不正アクセス禁止法違反 |
| 平成19年1月17日 | フィッシングを利用したオークション詐欺被疑者らの逮捕 | 被疑者らは、「フィッシング」により、他人のID・パスワードを入手した上、インターネットカフェから、入手したID及びパスワードで他人になりすまし、インターネットオークションで架空出品して、落札者から代金を騙し取りました。 | 不正アクセス禁止法違反<br>詐欺罪<br>私電磁的記録不正作出・同供用罪 |
| 平成18年11月29日 | 「ホームページ荒らしメンバー」らを不正アクセス禁止法違反等で検挙 | 被疑者らは、インターネット上の掲示板に書き込まれた他人のホームページのID・パスワードを用いて、同ホームページに不正アクセスし、内容を書き換えたり、閉鎖するなどの改ざん行為をしました。 | 不正アクセス禁止法違反<br>私電磁的記録不正作出・同供用罪 |

http://www.keishicho.metro.tokyo.jp/jiken/kenkyo/jiken.htm

Webroot Software, Inc.

# 警視庁ハイテク事件簿からのID盗難の事件 2

Privacy. Protection. Peace of mind.

| 検挙年月日 | 事案 | 内容 | 適用罪名、罰条 |
|---|---|---|---|
| 平成18年6月13日 | 元インターネットカフェ従業員を不正アクセス行為で逮捕 | 被疑者は、インターネットカフェ従業員の立場を利用し、店内のパソコンに「キーロガー」を仕掛け、他人のID・パスワードを不正に取得した上、その入手したID・パスワードを利用して、オークションサイトにおいて数十回不正アクセス行為を繰り返していました。 | 不正アクセス禁止法違反 |
| 平成18年5月30日 | フィッシング行為で14歳少年を書類送検 | 被疑者は、インターネットゲームサイトの会員に対して虚偽のメールを送り、同サイトのフィッシングサイトへアクセスさせ、ID・パスワード等を不正に入手し、同ID・パスワードを用いて、ゲームサイトにおいて不正アクセス行為を繰り返していた。<br>未成年のフィッシング行為の摘発は全国初。 | 不正アクセス禁止法違反<br>著作権法違反 |
| 平成18年1月28日 | フィッシングを利用したオークション詐欺被疑者の逮捕 | 被疑者は、大手オークションサイト利用者のID・パスワードを不正に入手することを企て、インターネットカフェからフィッシング行為を繰り返し、ID・パスワードを不正に入手しました。<br>そして、入手したID及びパスワードを使用して、同オークションサイトへ他人になりすまして不正にログインした上、商品券や旅行券などを落札して、出品者から商品を騙し取りました。 | 不正アクセス禁止法違反<br>詐欺罪 |
| 平成18年1月16日 | スパイウェアを使用したインターネットバンキングに対する不正アクセス禁止法違反等被疑者を逮捕 | 被疑者らは、スパイウェアを作成の上、某会社のネットバンキング用のID、パスワードを不正に入手して、他人の住居等の無線LANアクセスポイントを利用し、入手したID、パスワードを使い銀行のサーバに不正アクセスして、他人名義の口座等から自己が管理する口座に約1500万円を送金しました。 | 不正アクセス禁止法違反<br>電子計算機使用詐欺罪 |

http://www.keishicho.metro.tokyo.jp/jiken/kenkyo/jiken.htm

Webroot Software, Inc.

# 警視庁ハイテク事件簿からのID盗難の事件 3

Privacy. Protection. Peace of mind.

| 検挙年月日 | 事案 | 内容 | 適用罪名、罰条 |
|---|---|---|---|
| 平成17年10月24日 | 不正アクセス行為により個人情報を不正取得し転売した被疑者の逮捕 | 被疑者は、大手ネットショッピングモールを管理する会社のサーバコンピュータから他人の個人情報を取得することを企て、平成17年5月11日から同月14 日までの間、 前後27回にわたり、同人の所有するパソコンから、同モールの出店店舗に付されたユーザ名及びパスワードを入力し、不正アクセスの上、個人情報を不正に取得しました。 | 不正アクセス禁止法違反 |
| 平成17年6月13日 | フィッシングサイト開設による著作権法違反及び不正アクセス禁止法違反被疑者の逮捕 | 被疑者は、インターネットサービス会社の会員のログインID、パスワードの個人情報を不正に入手することを企て、同社がホームページとして公開している「ログイン画面」をコピーして、インターネット上に偽のホームページを公開し、パソコン及び携帯電話から同ログイン画面を閲覧した会員が誤信し、入力した ID、パスワードを不正に入手した上、自宅のパソコンから、入手したログインID及びパスワードを使用して、不正アクセス行為を行い、会員のメール等の個人情報をのぞき見ました。<br>フィッシング行為の摘発は全国で初めての検挙です。 | 著作権法違反<br>不正アクセス禁止法違反 |
| 平成17年3月22日 | 他人に成り済まして自殺予告メール等を送信した被疑者を、不正アクセス禁止法違反で検挙 | 被疑者は、平成16年12月、自宅のパソコンから、他人のIDとパスワードを使い会員になりすまし、インターネットサービスに接続して、その会員のメール アドレスから、「これから自殺しようと思っています。私のID及びパスワードは○○です。」などと記載したメールを、別のインターネットサービス会社の問 い合わせ窓口に送信していました。<br>被疑者は、ある掲示板で個人情報がネット上に流出しているとの情報を発見し、第三者のIDとパスワードを入手し、無断で使用していたものです。 | 不正アクセス禁止法違反 |

http://www.keishicho.metro.tokyo.jp/jiken/kenkyo/jiken.htm

Webroot Software, Inc.

# 売買されているオンラインアカウント

Privacy. Protection. Peace of mind.

Webroot Software, Inc.

# どのようにしてアカウントが盗まれる

Privacy. Protection. Peace of mind.

- 迷惑メールを使ってPhishingサイトに誘導
- トロイの木馬を使って、インストール
  - 最初にダウンローダのトロイを感染させる
  - ダウンローダが次のマルウェアをインストール

- ソーシャルエンジニアリングを使ったマルウェアの感染
  - SOEによる検索結果の利用
  - 掲示板への書き込み
  - SNSやブログへの書き込み
  - Wikiへの書き込み
  - 脆弱なサイトの改ざんした一般Webへの埋め込み
  - 感染したサイトオーナのホームページに埋め込み

# Pinchにより収集された情報の例

Privacy. Protection. Peace of mind.

This module contains e-mail passwords from The Bat! v1, 2 & 3

[redacted]
[Down] [Down]
[Down] [F5]
[Fájl kicsomagolása]

[Total Commander 7.0 public beta 1 - BBC International Forwarders B.V.]
[Delete]
[Total Commander]

ICQ

[Total Commander 7.0 public beta 1 - BBC International Forwarders B.V.]
This [Delete]
121 [Total Commander]

[Total Commander 7.0 public beta 1 - BBC International Forwarders B.V.]
[Up]

242

[Up]

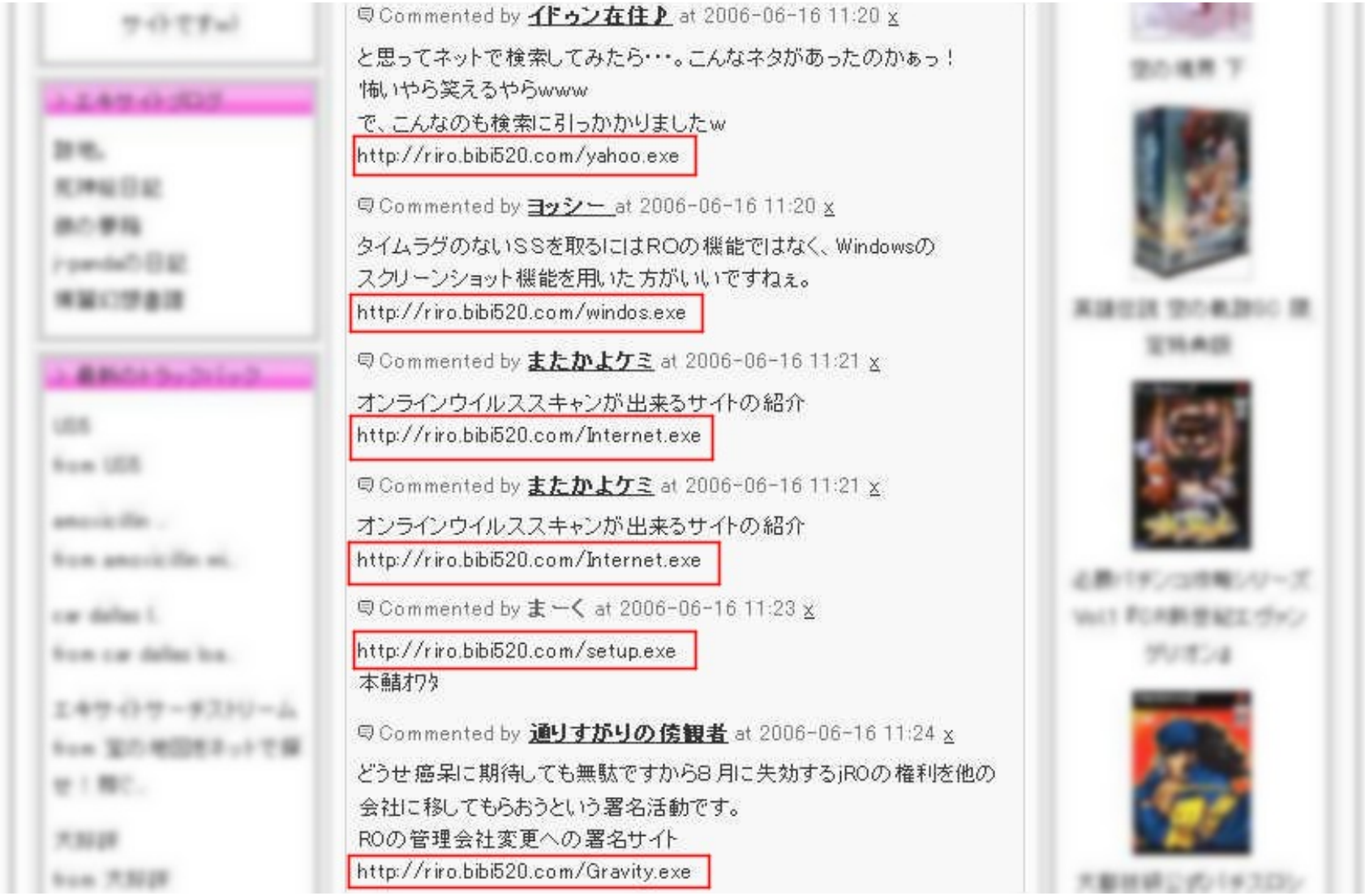
[Up]

[Up]
[Tab] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up]
251 [Up] [Up] [Up]
[Down] [Down] [Down] [Down] [Down] [Down] [Down] [Up]
[Down] [F5]
[Fájl kicsomagolása]

Webroot Software, Inc.

# トロイの木馬へのリンクを直接書き込み

Privacy. Protection. Peace of mind.



Commented by イドゥン在住♪ at 2006-06-16 11:20 x

と思ってネットで検索してみたら･･･。こんなネタがあったのかぁっ！
怖いやら笑えるやらwww
で、こんなのも検索に引っかかりましたw
http://riro.bibi520.com/yahoo.exe

Commented by ヨッシー at 2006-06-16 11:20 x

タイムラグのないSSを取るにはROの機能ではなく、Windowsの
スクリーンショット機能を用いた方がいいですねぇ。
http://riro.bibi520.com/windos.exe

Commented by またかよケミ at 2006-06-16 11:21 x

オンラインウイルススキャンが出来るサイトの紹介
http://riro.bibi520.com/Internet.exe

Commented by またかよケミ at 2006-06-16 11:21 x

オンラインウイルススキャンが出来るサイトの紹介
http://riro.bibi520.com/Internet.exe

Commented by まーく at 2006-06-16 11:23 x

http://riro.bibi520.com/setup.exe
本鯖オワタ

Commented by 通りすがりの傍観者 at 2006-06-16 11:24 x

どうせ癌呆に期待しても無駄ですから8月に失効するjROの権利を他の
会社に移してもらおうという署名活動です。
ROの管理会社変更への署名サイト
http://riro.bibi520.com/Gravity.exe

Webroot
SOFTWARE, INC.

# トロイの木馬をインストールする罠サイトへのリンクを書き込み

Privacy. Protection. Peace of mind.

640. **プロ北森の短剣脱衣** 返信 引用

名前: Eirのパンダ　日付: 1月26日(金) 9時39分

プロ北特化武器のリニューアル、CW1の取得、コンバーターの実装等で環境が色々変わったので|-`)っべたっ。

武器は＋9ディカーセイトハロウドギガンティックグラディウス

スキルはhttp://www.korunowish.com/897656/
やっとスタブに振り始めました。

大体15～30分ごとにプロ北力プラセーブで森との往復オンライン。
付与無しでマンティスBB
http://www.korunowish.com/897656/

639. **SEO/HPランクアッププログラム** 返信 引用

名前: Mapper64　日付: 1月25日(木) 20時40分

特殊な方法で
HPのランクアップを実現します。
まずはお問い合わせを。
そのほかにもさまざまなプランが
ございます。

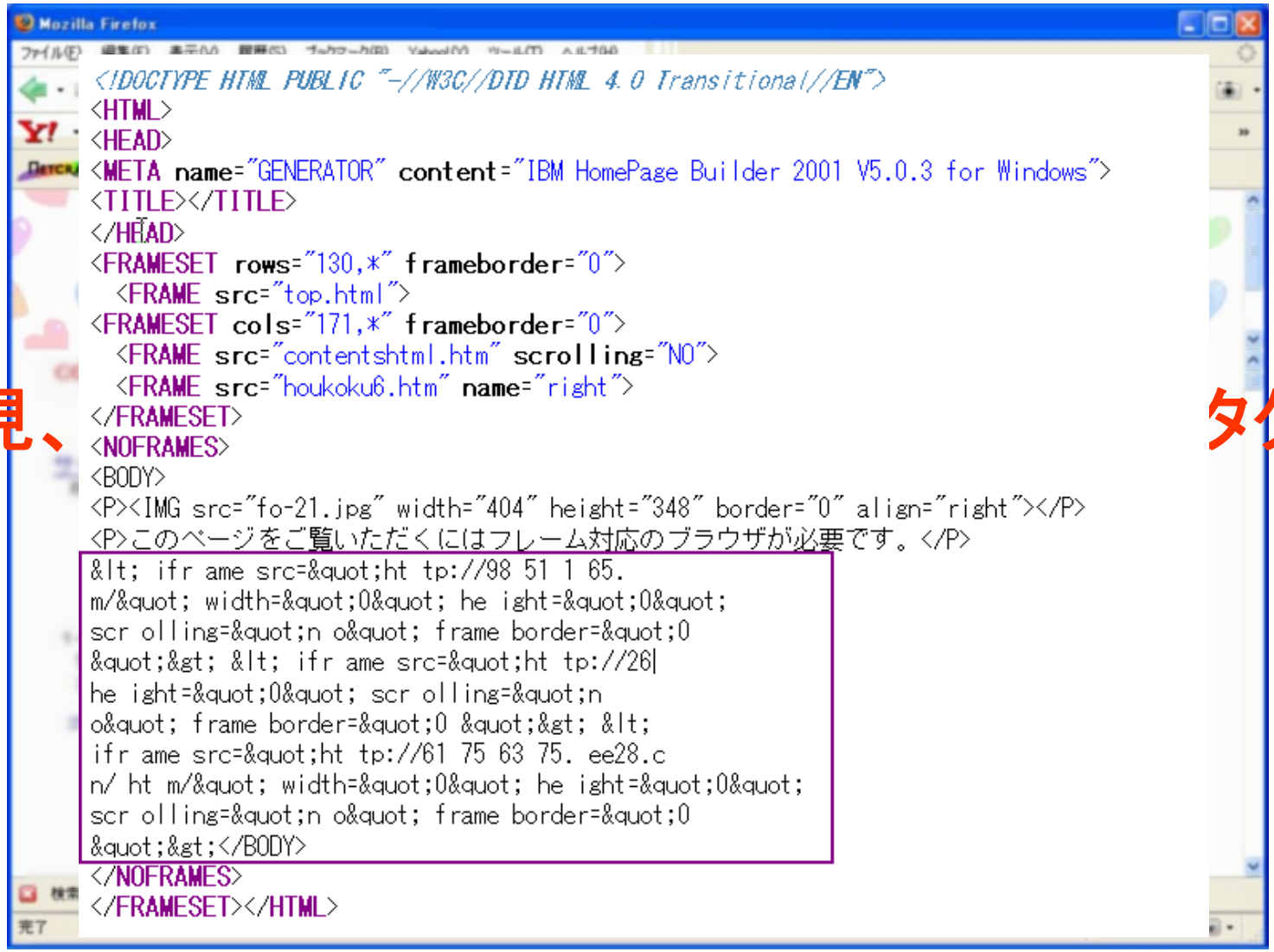
http://www.mapper64.com/
各種ソフト開発致します。

Webroot Software, Inc.

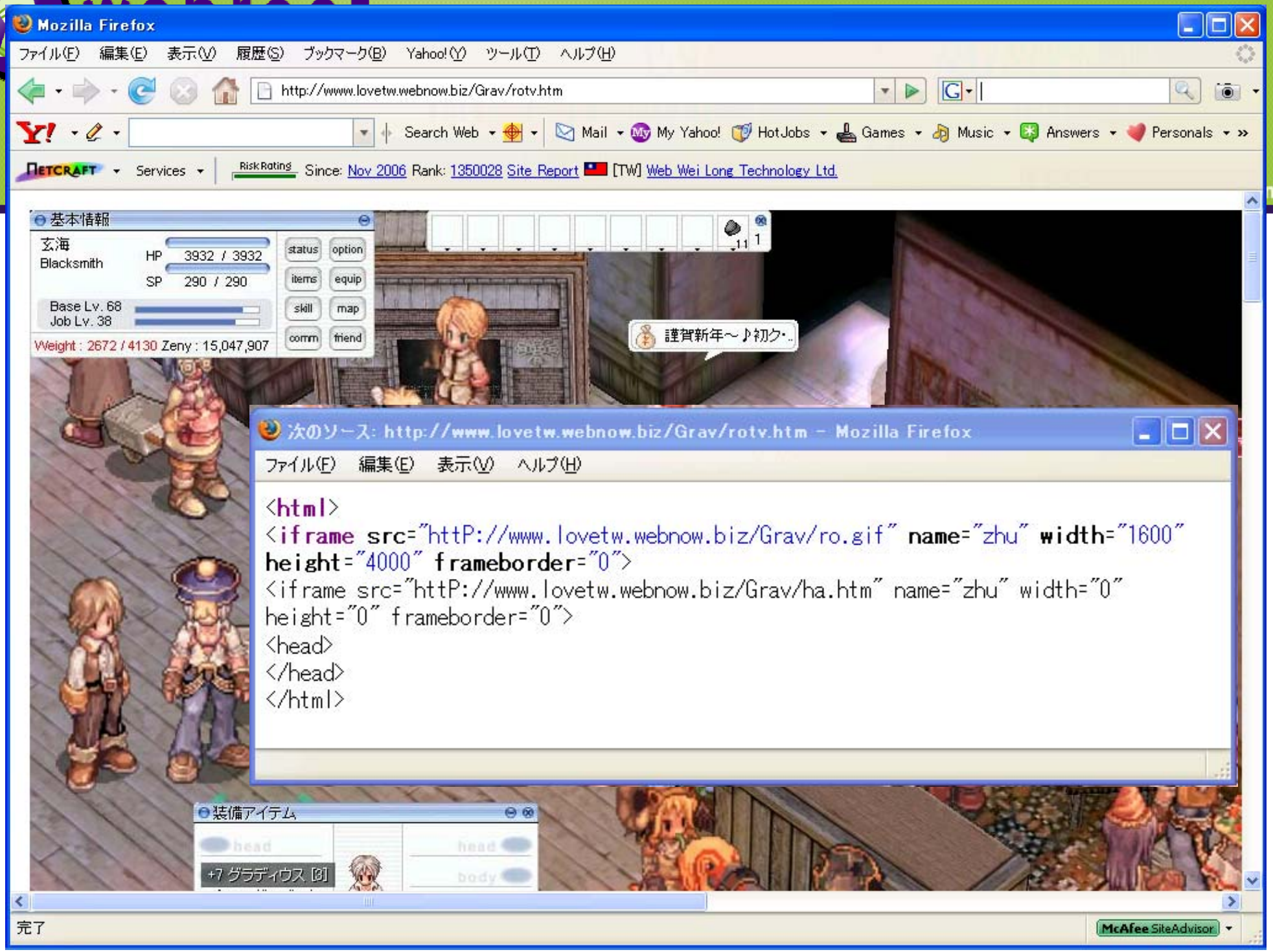
# トロイの木馬の感染を誘うページ

Privacy. Protection. Peace of mind.

一見、

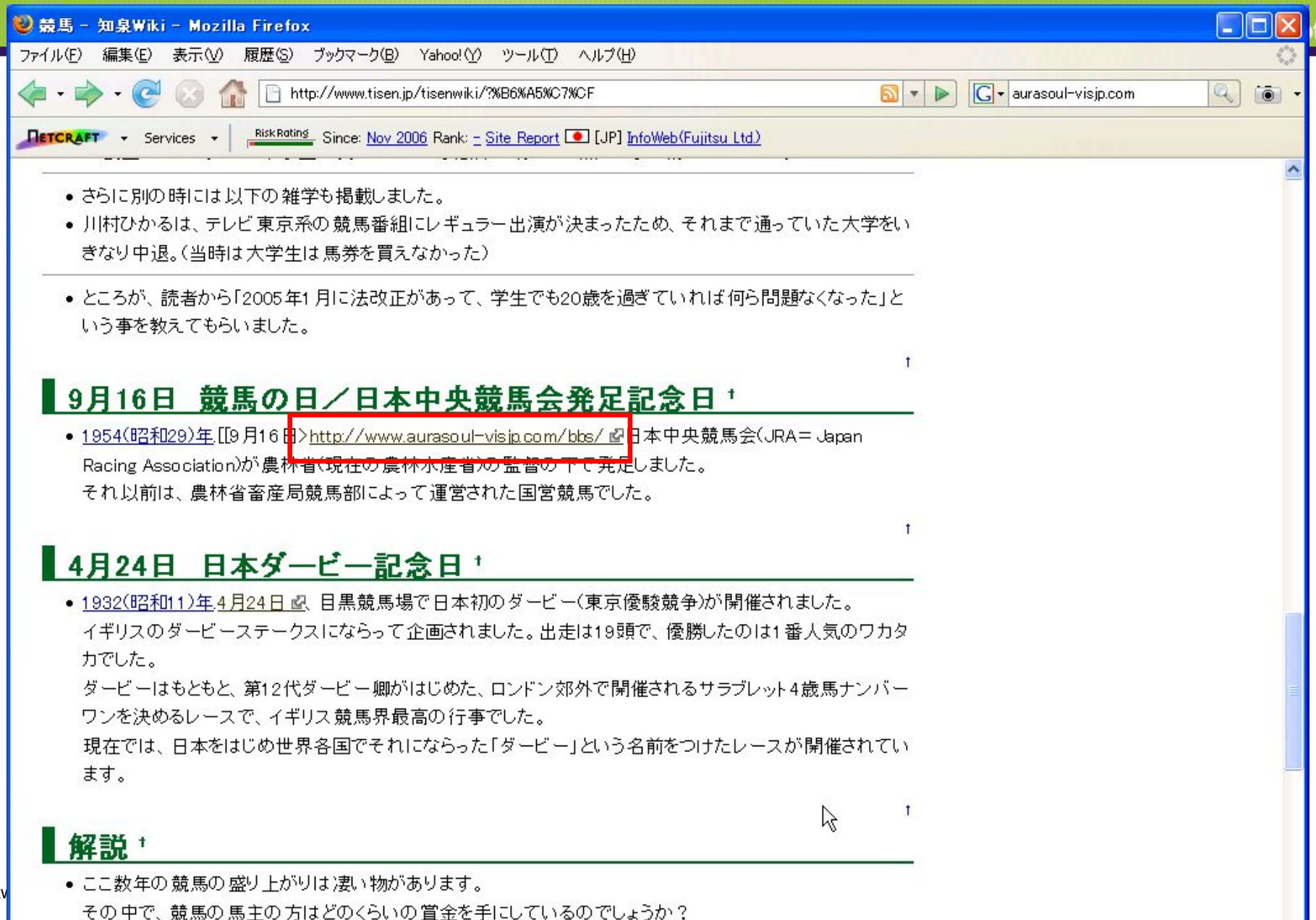



タグが挿入


Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) Yahoo!(Y) ツール(T) ヘルプ(H)
http://www.lovetw.webnow.biz/Grav/rotv.htm
Search Web Mail My Yahoo! HotJobs Games Music Answers Personals
NETCRAFT Services Risk Rating Since: Nov 2006 Rank: 1350028 Site Report [TW] Web Wei Long Technology Ltd.
基本情報
玄海
Blacksmith
HP 3932 / 3932
SP 290 / 290
Base Lv. 68
Job Lv. 38
status option
items equip
skill map
comm friend
Weight : 2672 / 4130 Zeny : 15,047,907
謹賀新年～♪初ク･･
次のソース: http://www.lovetw.webnow.biz/Grav/rotv.htm - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) ヘルプ(H)
<html>
<iframe src="httP://www.lovetw.webnow.biz/Grav/ro.gif" name="zhu" width="1600" height="4000" frameborder="0">
<iframe src="httP://www.lovetw.webnow.biz/Grav/ha.htm" name="zhu" width="0" height="0" frameborder="0">
<head>
</head>
</html>
装備アイテム
+7 グラディウス [3]
完了
McAfee SiteAdvisor

Webroot
SOFTWARE, INC.

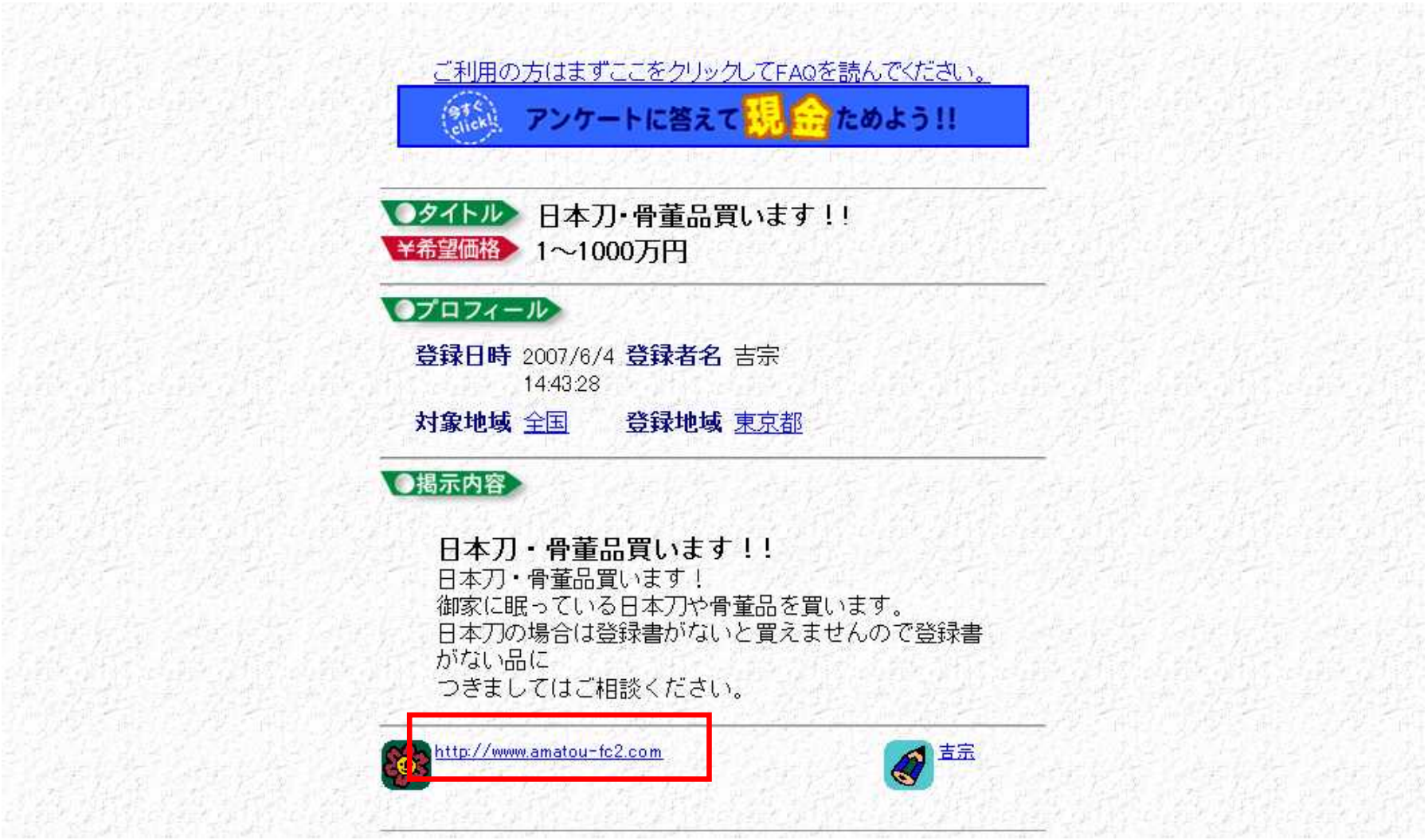
# オンラインゲームだけとは限らない



Webroot Software, Inc.

# あらゆるところに罠サイトが仕掛けられている

Privacy. Protection. Peace of mind.



# 従来のマルウェア対策の常識が通用しない現状

Webroot
SOFTWARE, INC.

# 日本のサイトもマルウェアを埋め込まれる改ざん

Privacy. Protection. Peace of mind.

Webroot Software, Inc.

# これまでのウイルスの常識が通用しない

Privacy. Protection. Peace of mind.

- 怪しいサイトでなくとも感染の危険性あり
- ウイルス対策ソフトの更新をきちんと行っていても感染の可能性あり

でも

- 怪しいサイトの方が改ざんの危険が高い
- ウイルス対策ソフトの更新をきちんと行っていれば、ダウンローダがダウンロードしてくる本体は検知される可能性が高い

よって、従来の対策も危険を減らすという意味では重要。
ただし、100%の安全は無いことを知っておく

Webroot Software, Inc.

# ユーザ側の対策

Privacy. Protection. Peace of mind.

- セキュリティパッチはきちんとあてる
- ウイルス対策、スパイウェア対策を行う。
- 怪しいWebサイトは訪れない。
- むやみにソフトウェアをインストールしない
- 掲示板やブログのコメントのURLを容易にクリックしない
- ログイン履歴をチェックする。
- 制限ユーザでInternetを利用する
- パスワードを定期的に変更
- **フィッシング等に関する情報の収集**

Webroot Software, Inc.

# パスワード対策について

Privacy. Protection. Peace of mind.

- 推測されにくいパスワードは当たり前。
  - パスフレーズを使う
    - Ex.
      .ha2sainoInu (ポチは二歳の犬）
      4649Onegaishi#（よろしくお願いします）
- 誰から自分のアカウントを守るのかで対策は変わる。
  - 身近な人に使われたくない。
    - 従来から言われるメモは危ない
  - Internetの先の犯罪者から守りたい
    - メモをしてでも頻繁に変える方が安全(たとえば、簡単な暗号を施してメモする）
- パスワード管理ソフトを使う

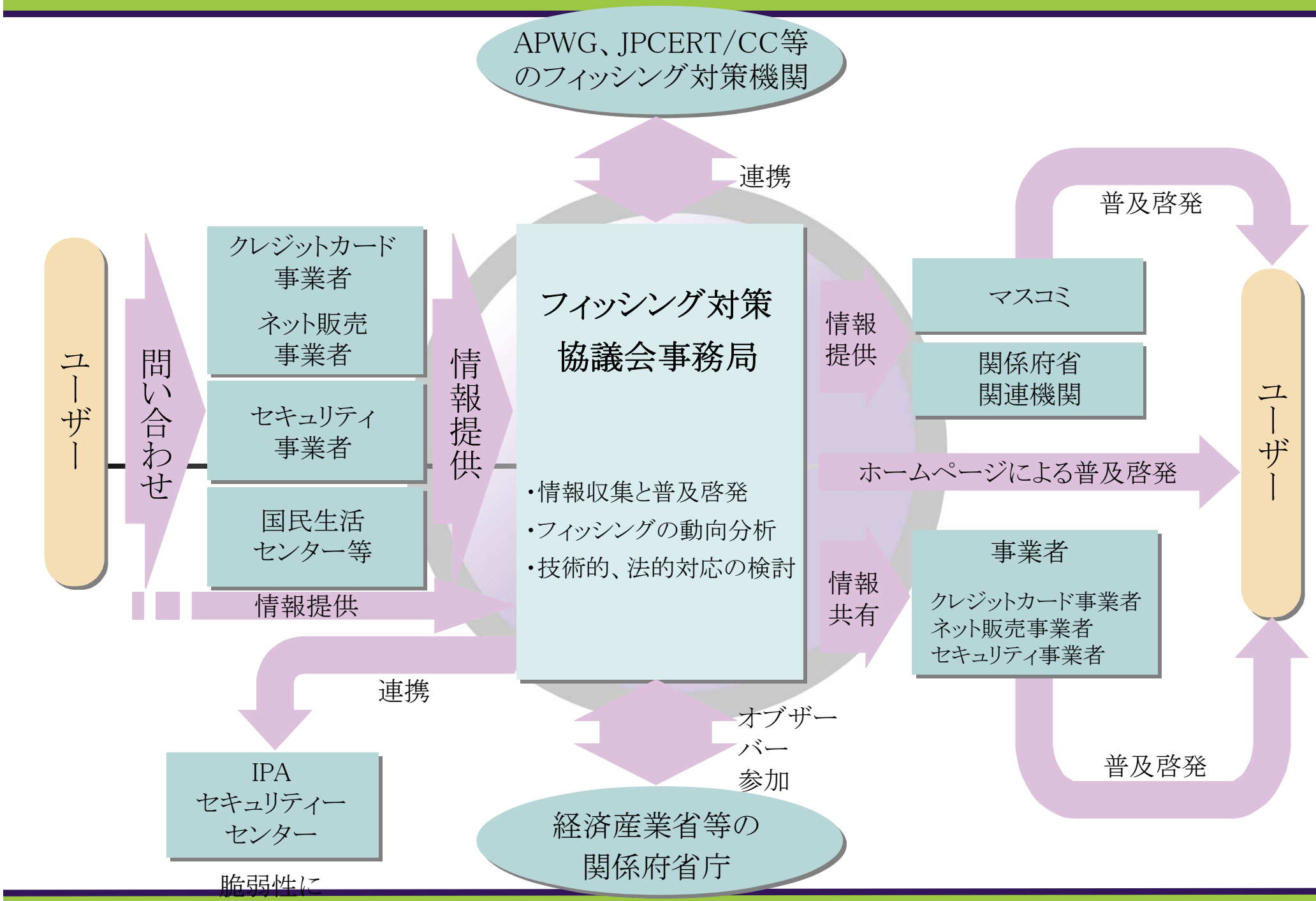
Webroot Software, Inc.

# 業者側の対策

Privacy. Protection. Peace of mind.

- 2要素認証など認証の強化
  - ワンタイムパスワードの利用
- ログインできるIPアドレスを限定する
  - 日本のユーザは日本国内からのみにアクセスを限定
- アクセス履歴をユーザに提供する
- 利用者へのセキュリティの教育・啓蒙
- 利用者へのセキュリティソフトの導入の義務化
- ユーザのアクセスの異常行動の検知を行う
- サイトのセキュリティを強固にするのは当然
- ID盗難の最新の情報の収集

# フィッシング対策協議会の役割


APWG、JPCERT/CC等
のフィッシング対策機関
連携
普及啓発
ユーザー
問い合わせ
クレジットカード
事業者
ネット販売
事業者
セキュリティ
事業者
国民生活
センター等
情報提供
フィッシング対策
協議会事務局
・情報収集と普及啓発
・フィッシングの動向分析
・技術的、法的対応の検討
情報
提供
マスコミ
関係府省
関連機関
ホームページによる普及啓発
ユーザー
情報
共有
事業者
クレジットカード事業者
ネット販売事業者
セキュリティ事業者
情報提供
連携
オブザーバー
参加
普及啓発
IPA
セキュリティー
センター
脆弱性に
関するもの
経済産業省等の
関係府省庁

Webroot Software, Inc.

# 2006年度の技術制度部会の成果のまとめ

Privacy. Protection. Peace of mind.

| ステップ | 内容 | 技術的対策方法 | 法･制度面での対策 |
|---|---|---|---|
| 0：フィッシングの準備 | 攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得 | 類似ドメイン取得の監視 | 類似ドメイン取得の禁止<br>JPRSによる類似ドメイン取得に関する注意喚起の提供 |
| 1：メールの送信 | フィッシングサイトに誘導するために詐欺メールの送信 | ISPによるメールフィルタリング技術<br>送信者認証、メールの電子署名<br>課題：迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知のとの見分けが付かない | 迷惑メール法、偽装メールに対する著作権法の適用<br>課題：迷惑メール法はフィッシングに対しては有効な歯止めとならない。<br>送信者認証や電子署名の技術を推進する制度が必要とされる。 |
| 2：ユーザがメールに反応 | 届いたメールを開封し、URLをユーザが実行 | 証明書付き電子メール | 教育・啓蒙活動によるユーザの教育<br>フィッシング対策協議会のWebによるフィッシングの啓蒙活動 |
| 3：フィッシング攻撃の実行 | 偽装サイトにユーザが訪れる | クロスサイトスクリプティングの脆弱性の除去 | 偽装Webに対する著作権法の適用 |
| 4：機密情報の送信 | 偽装サイトにユーザが個人識別情報を入力する | ユーザが容易にフィッシングサイトを見分けられるようにするための技術<br>フィッシング対策ツールバー<br>実在性も保証する厳密な証明書(EV SSL)<br>サイト画像認証<br>画像を利用したユーザ認証 | 制度面での技術の普及の後押しが課題 |
| 5：機密情報の入手 | 偽装サイト上の収集された個人識別情報をフィッシャーが取得 | マルウェアによる識別情報の盗み取りを防止する為、<br>ソフトキーボード、キーロガー検知 | 法制度の課題として、個人識別情報の入手を罰する手段がない |
| 6：機密情報の利用 | 個人識別情報を利用してユーザになりすましてサービスを利用 | 盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術<br>二要素認証<br>帯域外認証<br>課題：コスト | 不正アクセス禁止法<br>制度面での技術の普及の後押しが課題 |
| 7：不正行為の実行 | クレジットカードの利用や預金の引き落としなど不正行為の実行 | トランザクションの不正検知 | 現行の刑法に順ずる<br>課題：国際的な犯罪に対する国内法の限界 |

Webroot Software, Inc.

# 2007年度の成果の予定

Privacy. Protection. Peace of mind.

- フィッシング対策についてのガイドラインの策定
  - 事業者にとっての予防策
  - 事業者が被害に遭った(なりすまされた)場合の対応
  - 消費者が被害にあった場合の対応

# ありがとうございました！

http://www.webroot.co.jp/