Knight of Justice
WEB110
http://www.web110.com/

個人情報漏洩を防ぐための知識

愛媛県臨床衛生検査技師会
平成18年3月19日（日）13：00～15：00

WEB110代表　吉川誠司
http://web110.com/

Knight of Justice
WEB110
http://www.web110.com/

目次

1. サイバー犯罪の動向
2. 企業で発生する情報漏えいの分類
3. 個人情報漏えい事件の分析
4. Winnyからの情報漏えい
5. 盗難・紛失による情報漏えい
6. ウェブサイトからの情報漏えい
7. スパイウェア
8. フィッシング
9. ネットバンキング

1. サイバー犯罪の動向

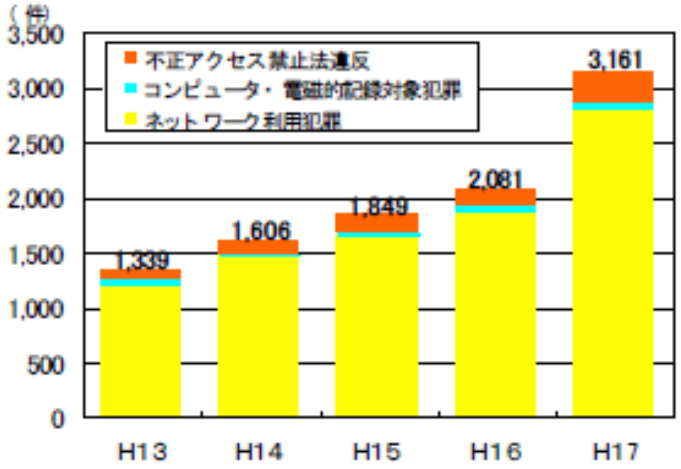
1　サイバー犯罪の検挙件数

サイバー犯罪（情報技術を利用する犯罪）の検挙件数は3,161件で、前年（2,081件）と比べて1,080件、51.9%増加。

（主な特徴）

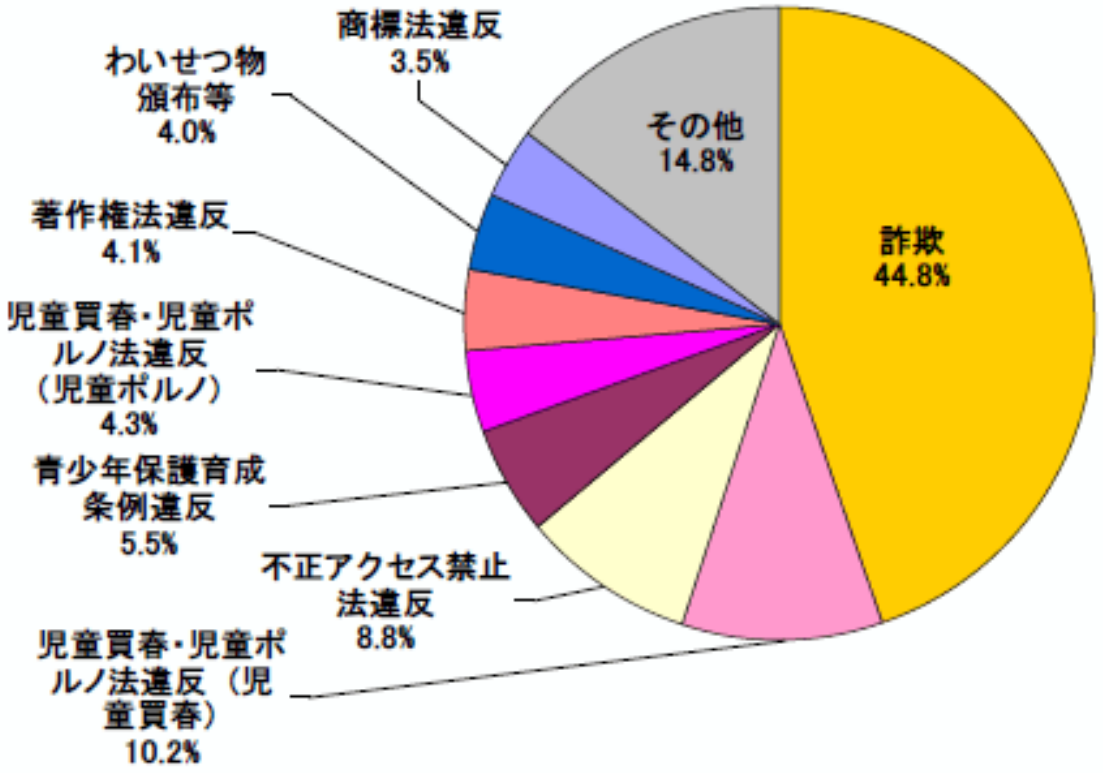
○　不正アクセス禁止法違反が、277件で前年の約２倍に増加した。

○　ネットワーク利用犯罪では、詐欺が1,408件で、前年の約2.6倍に増加した。その内訳は、インターネット・オークションを利用したものが多い。



1. サイバー犯罪の動向

平成17年　検挙事件の罪名別割合



1. サイバー犯罪の動向

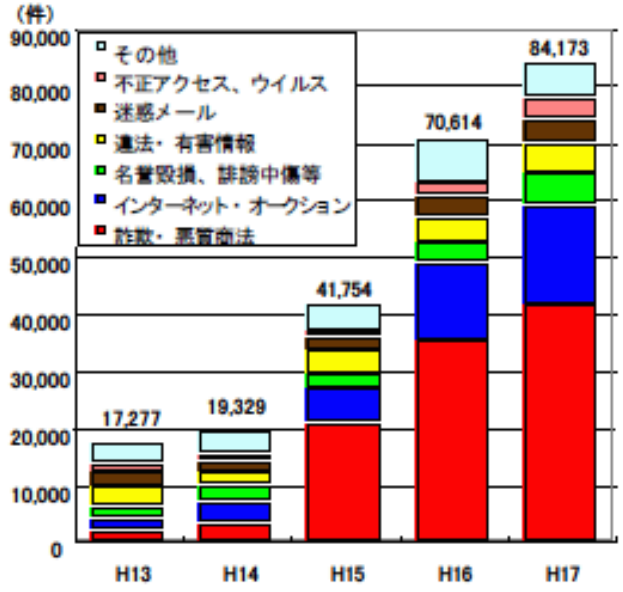
2　サイバー犯罪等に関する相談受理件数

都道府県警察のサイバー犯罪相談窓口等が受理した相談受理件数は、84,173件で、前年(70,614件)と比べて19.2%増加。

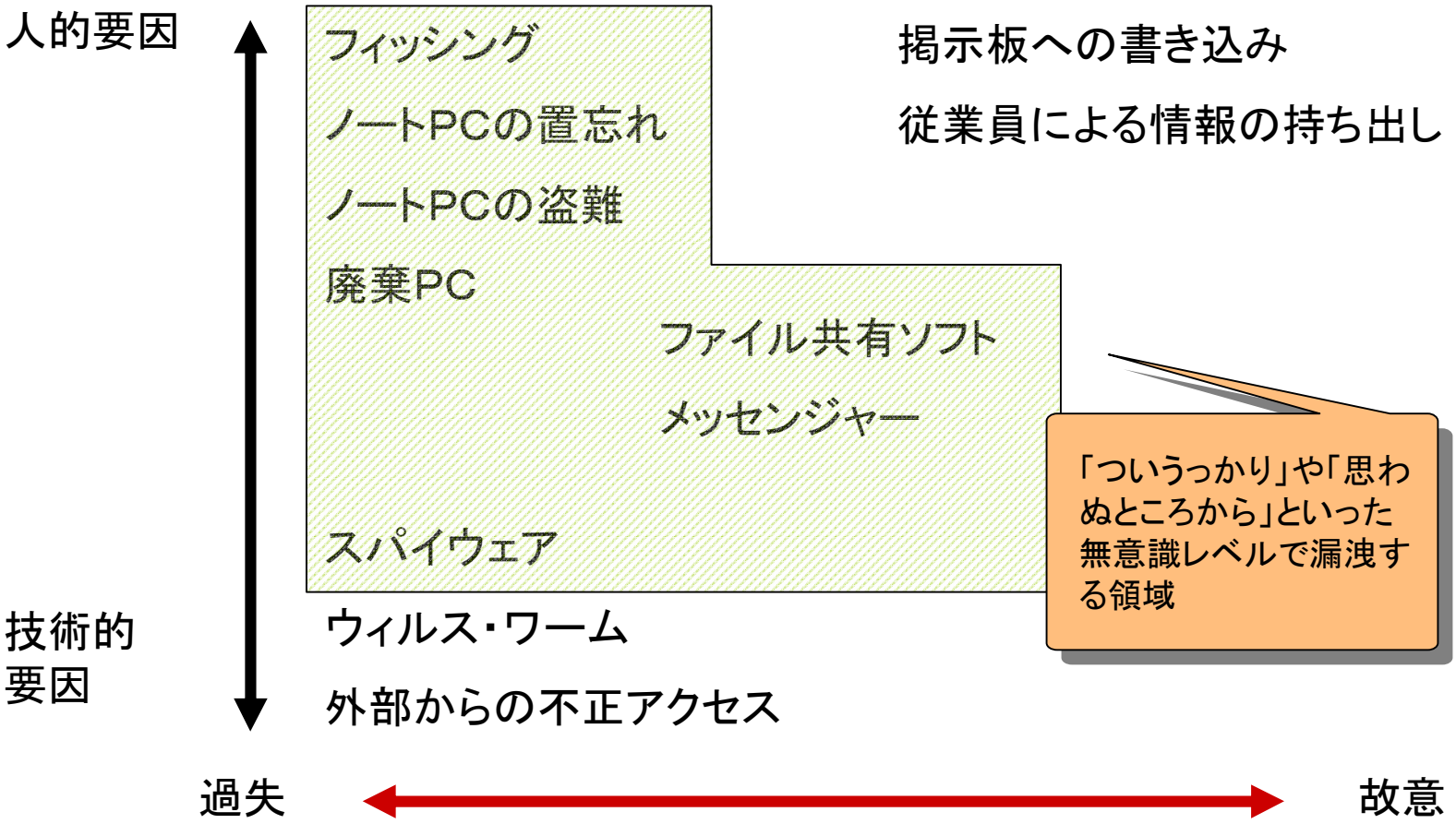
(主な特徴)

○ 詐欺、悪質商法に関する相談が約1.2倍、インターネット・オークションに関する相談が約1.3倍に増加した。

○ 不正アクセス、ウィルスに関する相談が約1.8倍に増加。オンラインゲームやオークションでの不正アクセスに関する相談が多い。



2. 企業で発生する情報漏えいの分類



3. 個人情報漏えい事件の分析

訴訟費用などの事故対応費用も発生する。さらには、企業イメージの低下による悪影響も発生。

	2002年	2003年	2004年
漏えい事件数	62件（55件）	57件（51件）	366件（336件）
損害賠償総額	189億2201万円	280億6936万円	4666億9250万円
最大損害賠償額	90億円	71億1990万円	542億円
平均損害賠償額	3億4403万円	5億5038万円	13億8897万円
総被害者数	41万8716人	155万4592人	1435万61人
最大被害者数	10万人	56万人	451万人
平均被害者数	7613人	3万482人	3万1056人

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

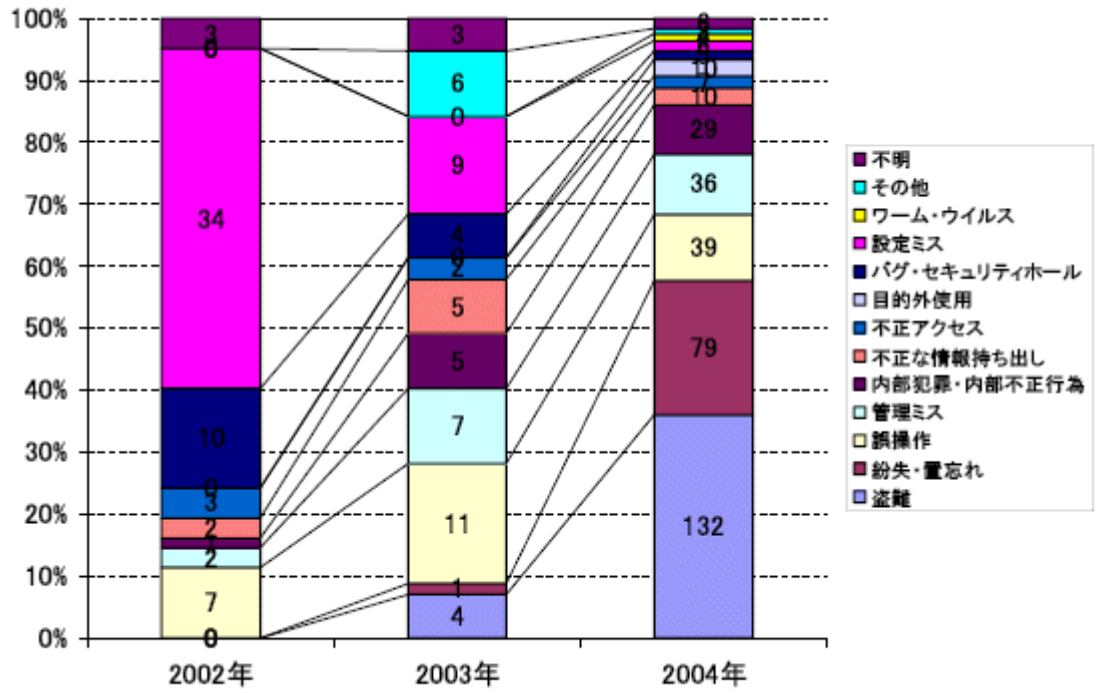
個人情報漏えい原因

情報漏えい原因	比率	情報漏えい原因	比率
盗難	36.15%	目的外使用	2.7%
紛失・置忘れ	21.6%	不正アクセス	1.9%
誤操作	10.7%	バグ・セキュリティホール	1.4%
管理ミス	9.8%	設定ミス	1.6%
内部犯罪・内部不正行為	7.9%	ウィルス・ワーム	1.1%
不正な情報持ち出し	2.7%	その他・不明	2.4%

盗難・紛失・置忘れだけで57.81%を占めている

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

情報漏えい原因の経年変化



「盗難」「紛失・置忘れ」が大幅に増加しているのは、それらのが個人情報漏洩事件として報道されたから。逆に、「設定ミス」「バグ・セキュリティーホール」の比率が下がっていることから、システム的な対策が浸透してきたことが伺える。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

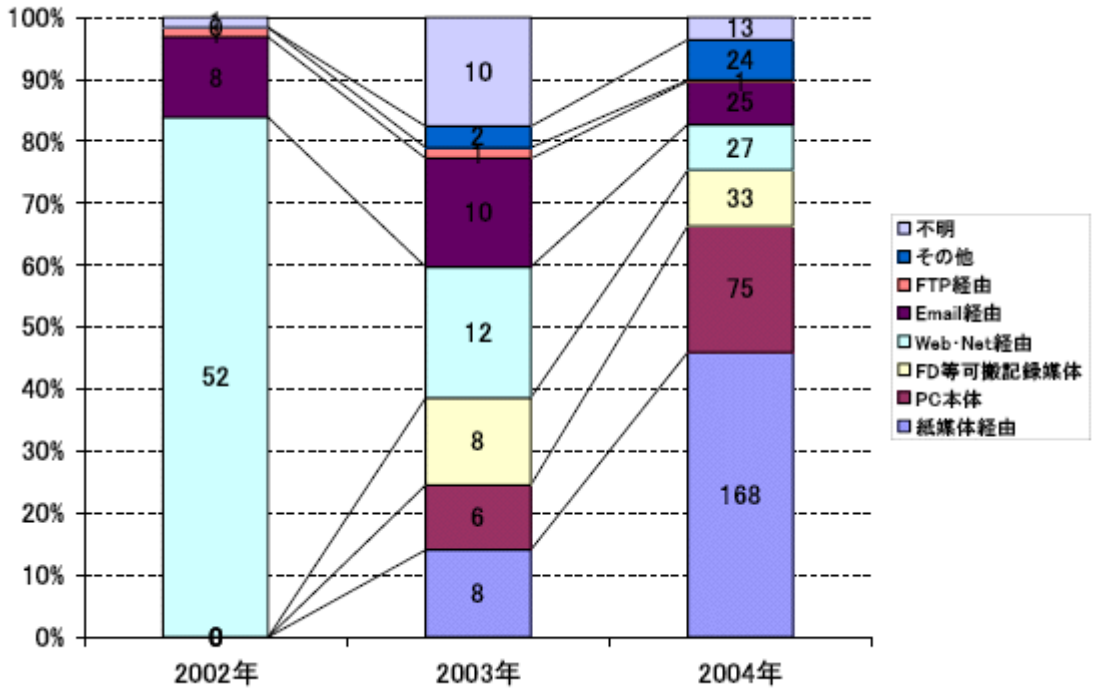
個人情報漏えい経路

情報漏えい経路	比率	情報漏えい経路	比率
紙媒体経由	45.9%	E-mail経由	6.8%
PC本体	20.5%	FTP経由	0.3%
FD等可搬記録媒体	9.0%	その他	6.6%
Web/net経由	7.4%	不明	3.6%

「紙媒体」「PC本体」「FD等可搬記録媒体」で75.4%を占めるのは、資料の入った鞄の盗難や車上荒らし、搬送中の紛失の発生率と連動しているため。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

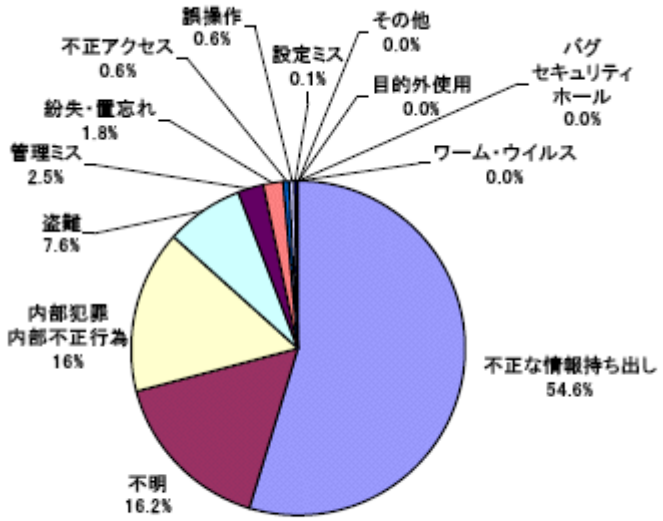
情報漏えい経路の経年変化



情報漏えい原因として「盗難や紛失」が増加したことに連動して「紙媒体」「PC本体」の比率が増加している。一方、システム的な対策が進んだことにより「web・net経由」での漏洩は減っている。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

情報漏えい原因別　被害者数の比率



原因別の被害者数の比率

情報漏えい原因の比率としては「内部犯行・内部不正行為」「不正な情報持ち出し」が合わせて10.6%であったのに対し、被害者数の比率では70.6%を占める。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

Knight of Justice
web110
http://www.web110.com/

4. Winnyからの情報漏えい

2006/3/16・・・愛媛県警、Nシステム情報流出か　車10万台ナンバー
2006/3/15・・・空港の暗証番号流出、全日空機長の私物パソコンから
2006/3/15・・・TBS出演者らの個人情報、「ウィニー」通じ流出
2006/3/14・・通知表80人分がネット流出・大津の教諭、ウィニー使う
2006/3/8・・・NTT西でも顧客情報流出
2006/3/8・・・住友生命、8000人分の個人情報流出
2006/3/7・・・愛媛県警　被害者情報や殺人事件資料流出
2006/3/5・・・岡山県警で1500人の捜査情報流出　被害者名など
2006/3/1・・・海自の情報流出、昨年中に「秘」含む5件　空自でも
2006/2/24・・・書記官PCから東京地裁の個人情報流出
2006/2/22・・・受刑者情報の流出、5施設3380人分と判明
2006/2/1・・・郵便局の顧客情報2800件、「ウィニー」通じ流出・千葉県
2006/1/27・・・広島の病院、ネットにデータ流出
2006/1/17・・・三井住友海上、業務委託先で590人分の個人情報漏洩
2006/1/16・・・7300人の個人情報流出　兵庫県養父市のCATV
2005/12/27 ・・・NEC子会社から顧客情報流出、社員の個人用PCから
2005/11/14・・・北海道職員ら約3500人分の個人情報がネット流出か
2005/10/7・・・アフラック、契約者564人分の個人情報がネット上に流出
2005/4/7…鳥取大学医学部付属病院、小児科の患者8人分の診療記録が流出
2005/4/1…鳥取赤十字病院、小児科の診療記録63人分が、インターネット上に流出
2005/3/29…東京医科歯科大学医学部付属病院の患者50人分の検査データが流出

Knight of Justice
web110
http://www.web110.com/

Winnyによる情報漏えい対策

Winnyによる情報漏えいを防止するために（**IPA**）
http://www.ipa.go.jp/security/topics/20060310_winny.html

1. 漏えいして困る情報を取り扱うパソコンには、Winnyを導入しない。
2. 職場のPCに許可無くソフトウェアを導入できないようにする。
3. 職場のPCを外部に持ち出さない。
4. 職場のネットワークに、私有PCを接続しない、またはできないようにする。
5. 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する。
6. 職場のPCからUSBメモリやCD等の媒体に情報をコピーできないようにする。
7. 漏えいして困る情報を許可無くメールで送らない、または送れないようにする。
8. ウイルス対策ソフトを導入し、最新のウイルス定義ファイルで常に監視する。
9. 不審なファイルは開かない。
10. 職務上のデータを私有のPCに保存しない。させない。

Knight of Justice
web110
http://www.web110.com/

5. 盗難・紛失による情報漏えい

- 障害者雇用報告書2183社分を紛失・厚労省
- 酒田天然ガス、顧客情報委託先が410件を含むメモリーカード紛失
- 日清食品、約300名分の履歴書や個人情報を含むパソコン盗難
- 岐阜スズキ販売、車上荒らしで個人29名と業者15店の顧客情報を含む鞄盗難
- 益田市、387件の顧客情報を含む水道検針端末用メモリカード紛失
- 交番の連絡簿を紛失、170世帯の個人情報入り・京都府警
- 金融機関の個人情報紛失、287機関で計678万件に
- 中学生の個人情報入ったパソコン盗難・神奈川県平塚市
- 東大、約2100人分の学生個人情報納めたパソコン盗難
- みずほ銀、新たに4万7000人分の個人情報紛失が判明
- りそな銀、3万件以上の顧客情報を紛失
- 大分銀、顧客情報13万1000人分を紛失
- NHK沖縄放送局、「沖縄戦の絵」提供者290名の個人情報を含むPC紛失
- IMJビジネスコンサルティング、メール500件を含むPC紛失
- 東芝コンシューママーケティング、メールアドレスを含むPCの盗難2件
- 積水ハウス、車上荒らしで3邸分の顧客情報を記載した図面など盗難
- シティケーブルネット、車上荒らしで12世帯分の書類盗難
- 30万人分の個人情報入りPC盗難・花博の展望塔会員名簿
- がん患者約2000人の個人情報入りPC、横浜の医師宅で盗難
- JTB、個人情報1594人分が入ったノートパソコン紛失
- 全日空、個人情報約7000件を紛失
- あいおい損保、顧客情報7945件を紛失
- 虎の門病院で情報流出、医師がタクシーにメモリー忘れる

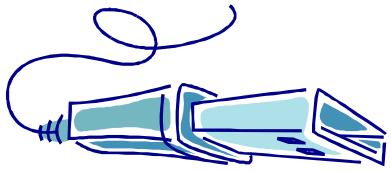
5. 盗難・紛失による情報漏えい対策

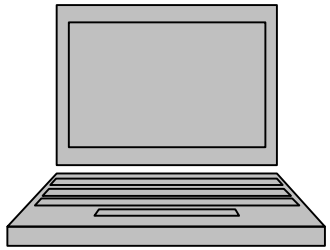
（1）ハードディスクレスPCの導入

参考：日立　FLORA Se210シリーズ

5．盗難・紛失による情報漏えい対策

（2）USBメモリと、それに付属している暗号ソフトの併用による　ノートPCのデータ保護

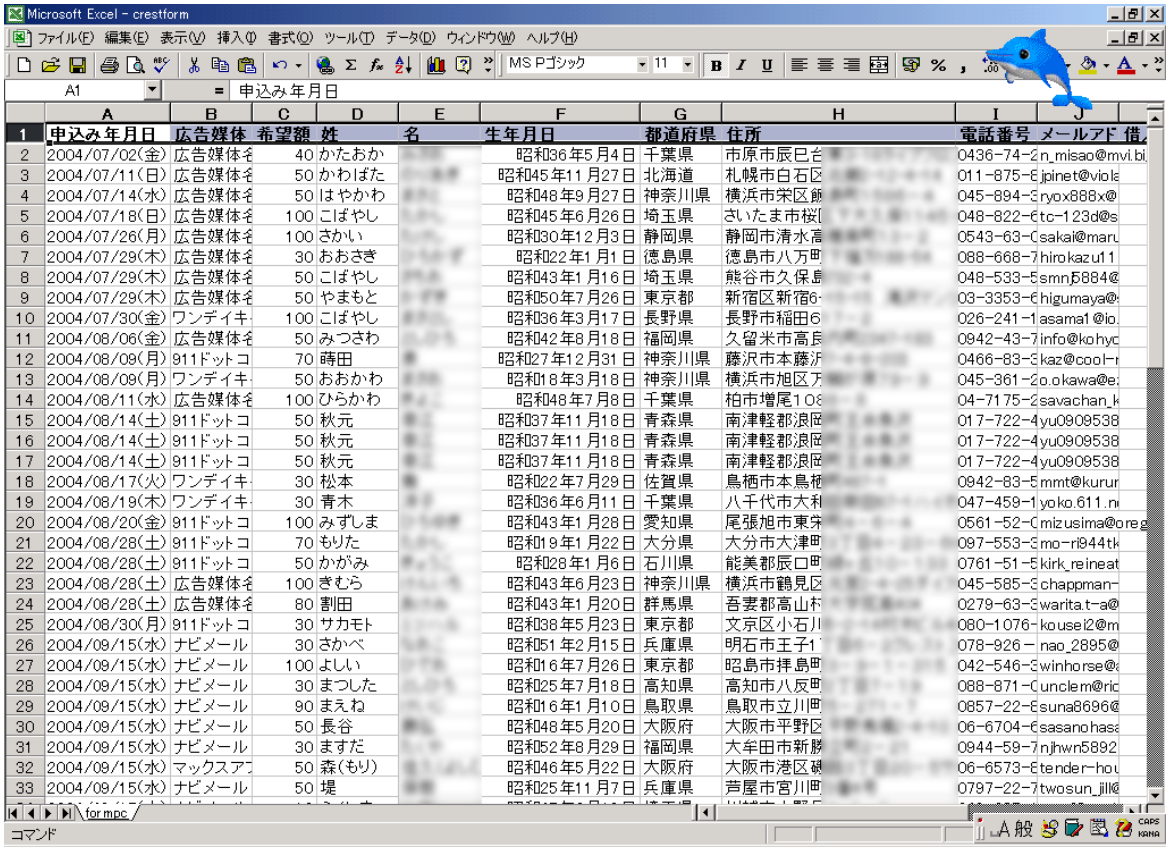




暗号化されたファイルはノートPCとUSBに2分割して保管する。移動する時には、ノートPCを鞄に入れ、USBメモリはキーホルダーに取り付け身につける。これならノートPCだけ盗まれても、個人情報をノートPCだけで復元することは難しい。

6. ウェブからの個人情報漏えい

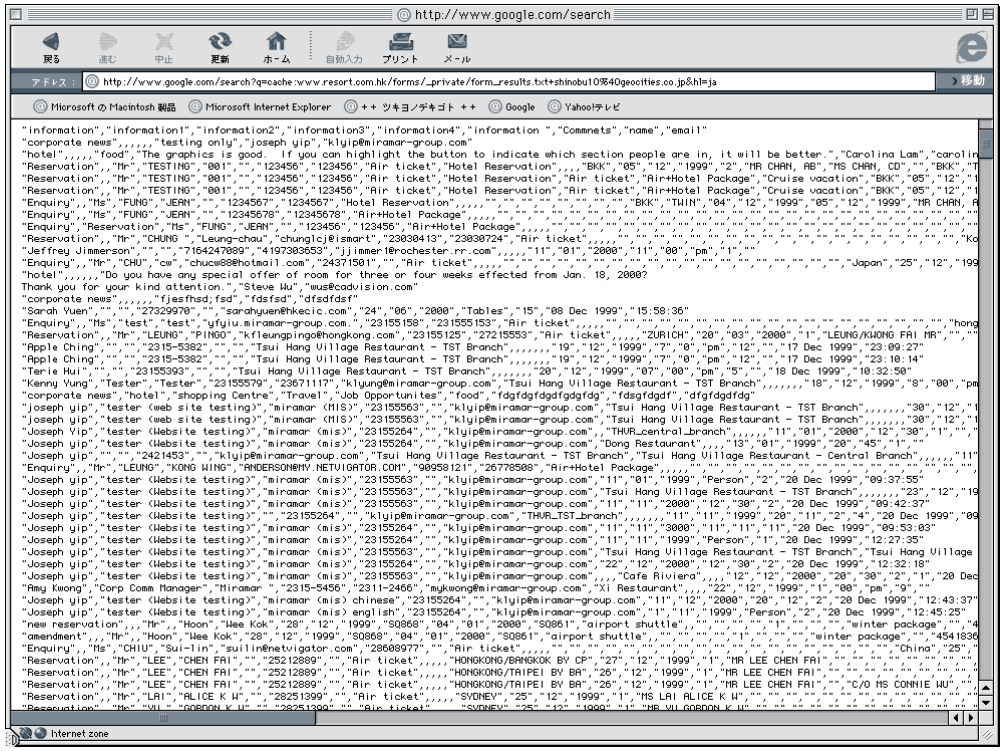
消費者金融サイトの顧客ファイルがブラウザで閲覧可能だった例



Knight of Justice
web110
http://www.web110.com/

6. ウェブからの個人情報漏えい

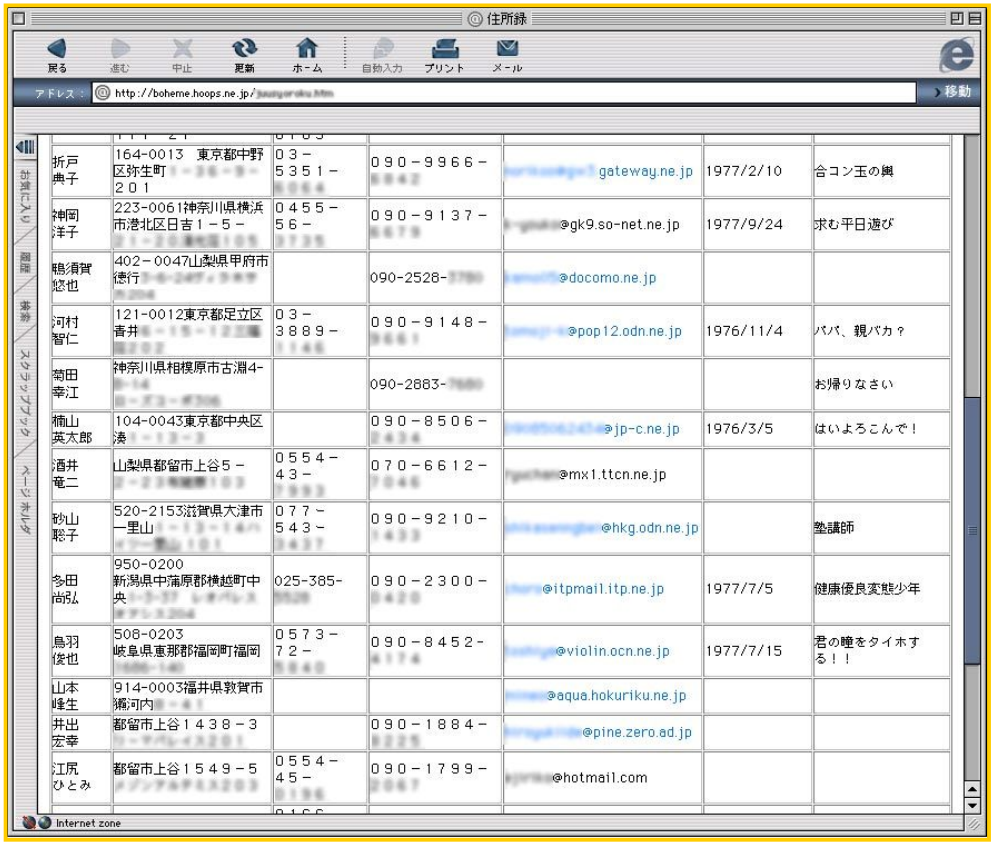
ホテルの顧客データがグーグルにヒットした例



自分の個人情報をキーワードにして検索してみましょう

6. ウェブからの個人情報漏えい

「サークル　名簿」で試してみると‥



（1）検索ロボット対策

①METAタグによるロボット対策

インデックスさせたくないHTMLファイルの<head>と</head>の間にMETAタグを挿入する

（1）検索ロボット対策

METAタグの挿入例（途中改行は入れない）

- 当該ページと、そこからリンクしている全てを検索対象からはずす

```
<meta name="ROBOTS" content="NOINDEX, NOFOLLOW">
```

- 当該ページのみを検索対象とし、その先のリンクを辿らないようにする

```
<meta name="ROBOTS" content="INDEX,NOFOLLOW">
```

- 当該ページは検索対象に載せず、そこからのリンクだけをたどるようにする

```
<meta name="ROBOTS" content="NOINDEX,FOLLOW">
```

- 当該ページをキャッシュをさせない

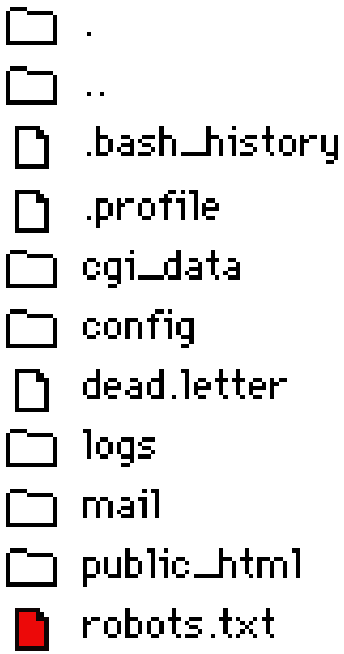
```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

Knight of Justice
WEB110
http://www.web110.com/

（1）検索ロボット対策

②robots.txtの設置による対策

制限内容を書いたテキストファイルをrobots.txtという名前で作成し、ルート・ディレクトリへアスキーモードでアップロードしておく。



（1）検索ロボット対策

全てのロボットに対して当該ディレクトリ以下をクロール対象から外す場合の記述例

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /tmp/
Disallow: /private/
（空白行）
```

（1）検索ロボット対策

③「.htaccess」によるrobot対策

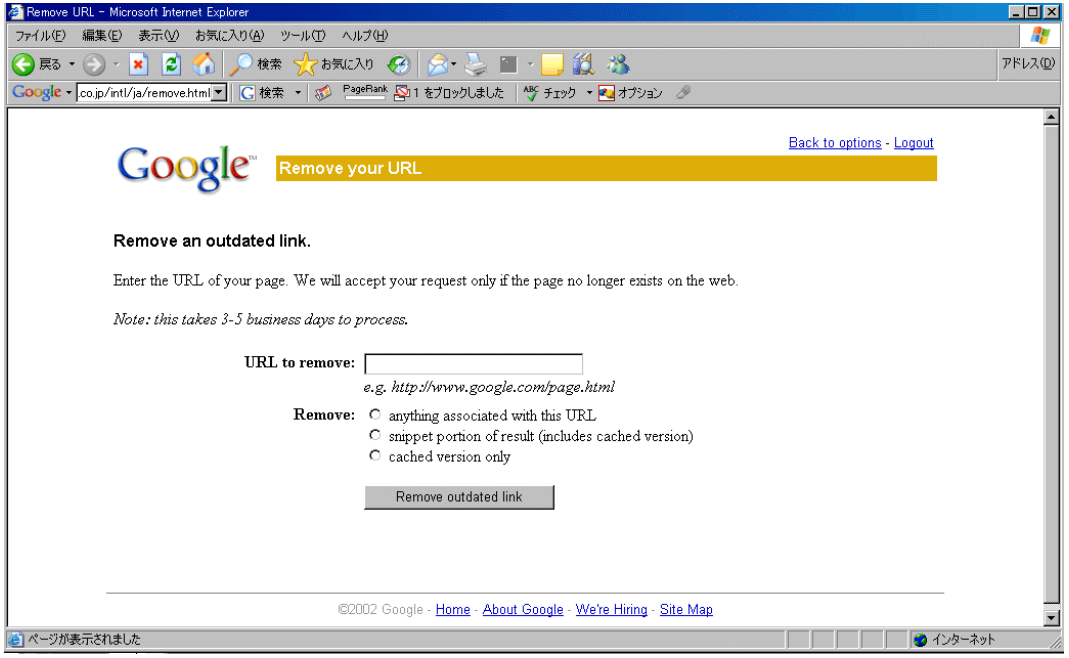
「robots.txt」を読まない、読んでも無視するロボットに対しては、
「.htaccess」でアクセス制限をする。

```
<Files *>
order allow,deny
allow from all
deny from 61.115.195.180
</Files>
```

Googleのキャッシュから削除する方法

「URL 自動削除システム 」を使用する。ただし事前に元のファイルをサーバーから削除しておく必要がある。

http://www.google.co.jp/webmasters/remove.html



7. スパイウェア

- 善良なプログラムファイルと見せかけて、その中に各種の個人情報収集機能を埋め込んだマリシャスソフトウェアの一種。
- 無料で配布されているソフトウェアの中に埋め込まれていたり、メールに添付されて送りつけられてくる。

スパイウェアの主な活動

- スクリーンキャプチャ・・・パソコンのデスクトップのスナップショットを撮る
- 特定のキーロギング・・・キーボードの打鍵内容をファイルに記録
- 行動分析・・・クリップボードのモニタリング、ブラウザの訪問履歴、クッキーファイルに保存された情報、キャッシュに保存されたパスワードを列挙して捕捉
- 特定の単語の認識・・・例えばクレジットカード番号やネットバンキングのURL、メールアドレスなど、一定の規則性を持った文字列が入力された場合にその内容を記録。
- ターゲットのIMウィンドーからメッセージを送信
- ウェブカメラのコントロール

進化するスパイウェア

「ホステージ・テイカー」

駆除するとPCのシステムを破壊する

「ルートキット」と呼ばれる技術で作成されたスパイウェアは、OS内部に入り込み、システムレベルで権限を不正に取得して、一般的なユーザーでは検出・駆除ができなくなる。

「ウォッチャー」

2つ1組の形でPCに侵入して、互いに監視し合い、一方が削除されるともう一方が復活させる。このタイプも完全に駆除するのが難しい。

ブログがスパイウェアの配布に悪用される

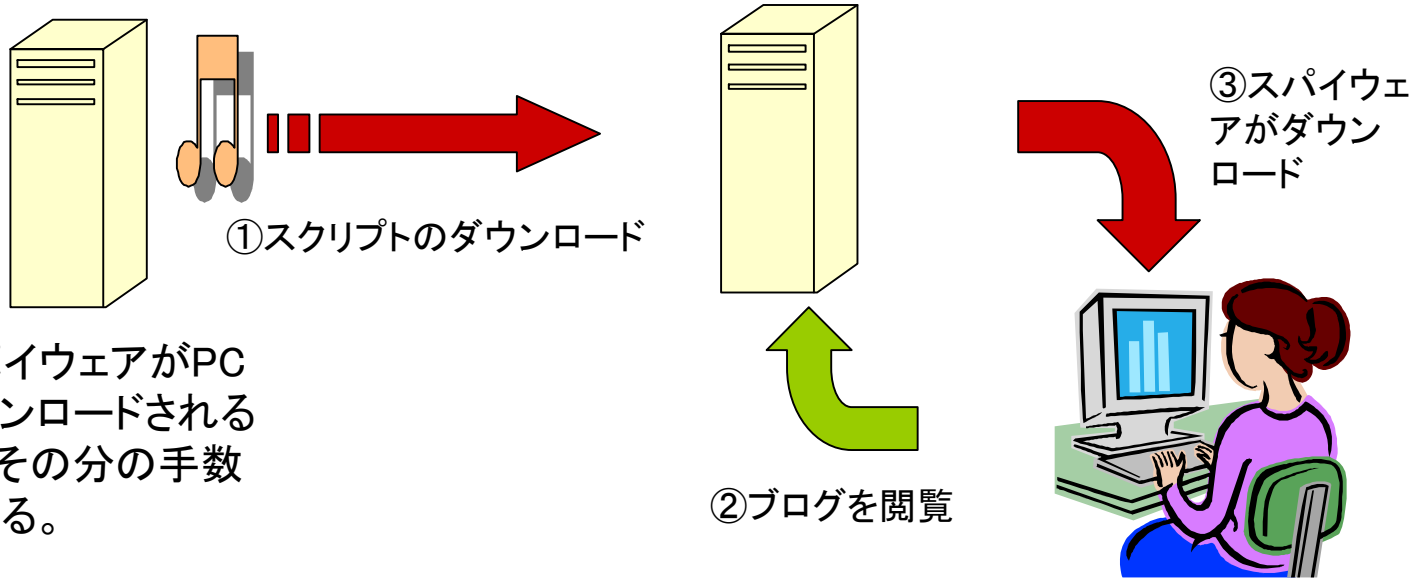
脆弱なウェブブラウザでブログにアクセスしてきたユーザーのPCに、
JavaScriptやActiveXを使って自動的にスパイウェアを送りつける手口。

iWebtunes

音楽再生機能等でサイトを強化するスクリプトを無償配布

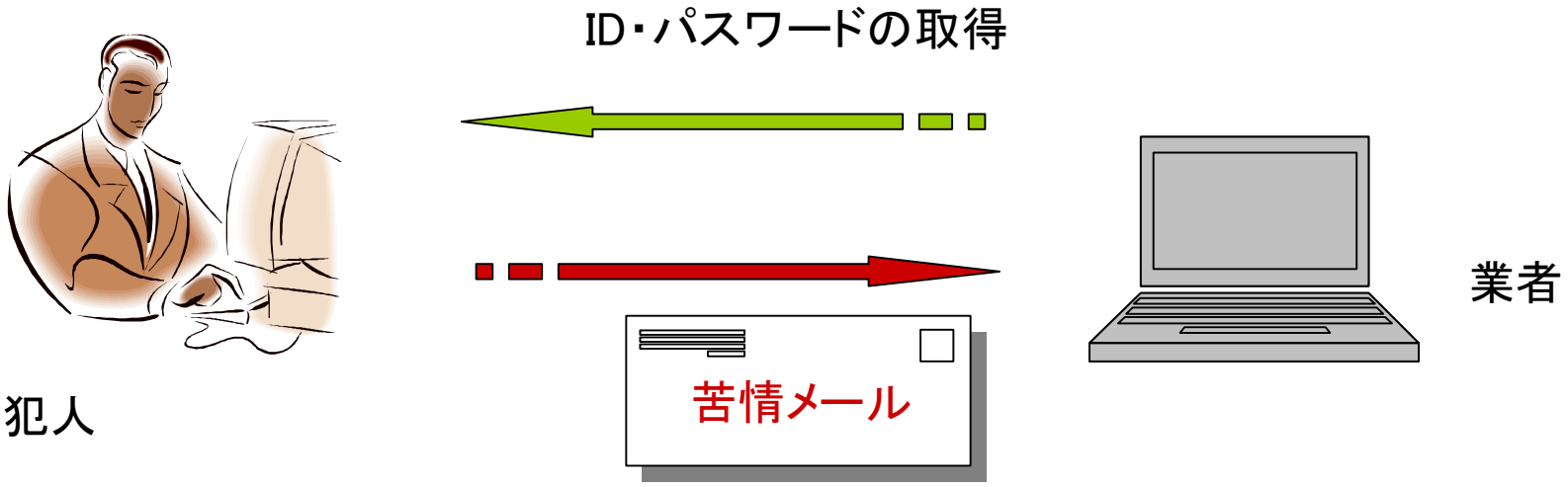
ブログサイト

GoogleのBlogger



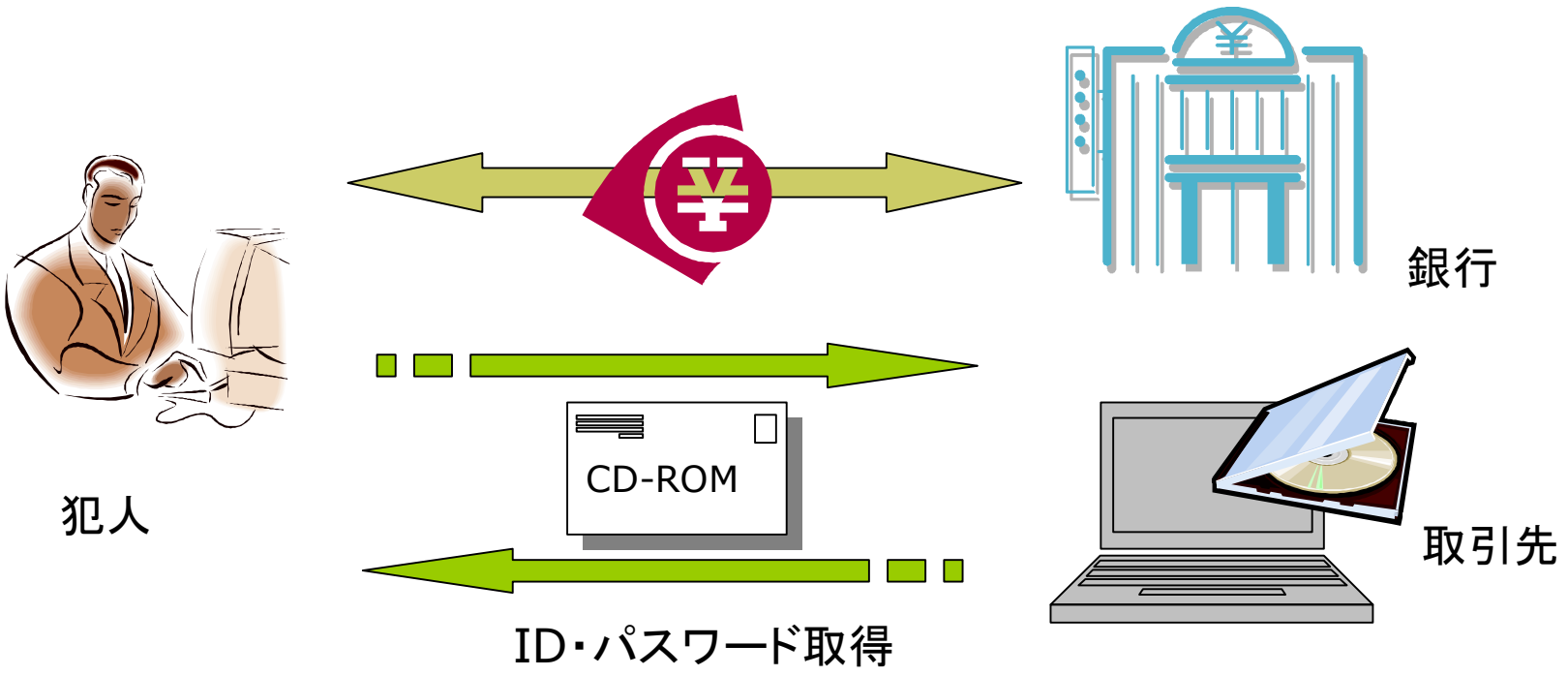
メールでスパイウェアを感染させる手口

- 容疑者はスパイウエアを自ら作り、楽天市場などの出店業者に客を装って約600通のスパイウェア添付メールを送付。10業者からネットバンキングの IDとパスワードを入手していた。業者がメールを開かざるを得ないようにするため、件名を「苦情」などとし「不良品だった。添付ファイルの写真を見て」と書き込んでいた。不正に入手した出店業者のIDとパスワードを利用し、業者の10口座から約1140万円を、自分たちが管理する口座に移していた。（2005年11月11日 ）



CD－ROMでスパイウエアを感染させる手口

- 2005年10月から11月にかけ、千葉銀行、北陸銀行、城北信用金庫の3金融機関を送り主と偽ったCD－ROMが顧客や取引先に郵送され、インストールした取引先の一部が不正送金の被害に遭う事件があった。



スパイウェア専用対策ソフト

Spy Sweeper 4.5J（ウェブルート・ソフトウェア）

http://webroot.com/jp/

- 高度化して検出・駆除ができないスパイウェアを1回のスキャンで完全に駆除できるという優位性があるという。
- 11月下旬からベクターなどのウェブサイトから3990円でダウンロード販売予定。

スパイウェア専用対策ソフト

スパイウェアの除去とインストール防止

SG AntiSPY

株式会社アークン

http://www.junglejapan.com/products/sec/aspy/index.html

スパイウェア専用対策ソフト

スパイウェアの除去とインストール防止

Spybot Search&Destroy1.4（フリー）

ダウンロード：http://cowscorpion.com/Antispy/spybot.html

Knight of Justice
web110
http://www.web110.com/

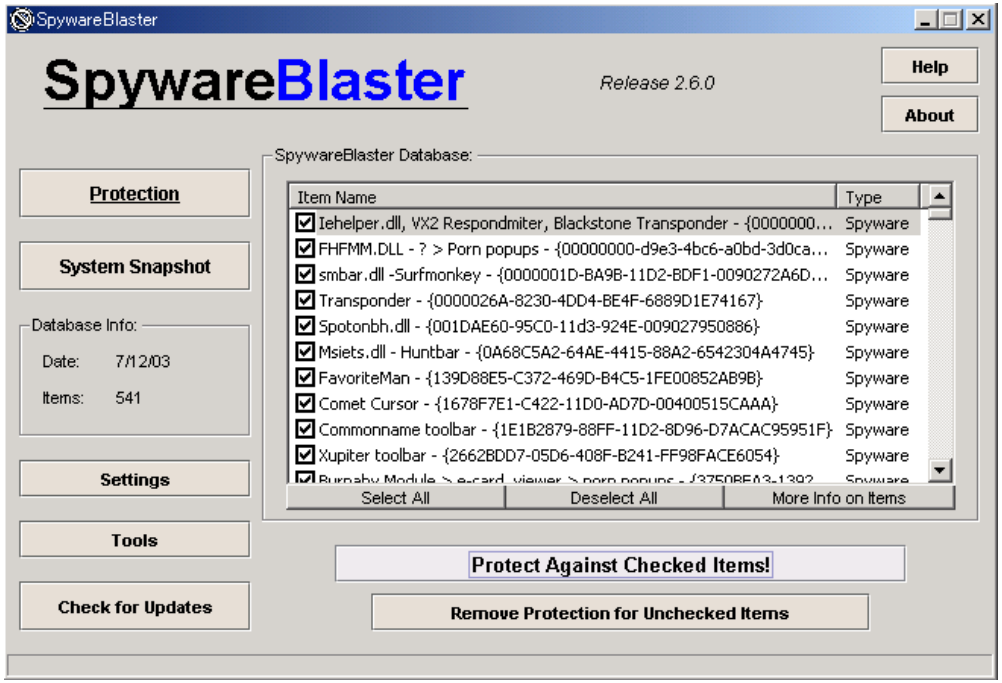
スパイウェア専用対策ソフト

スパイウェアがインストールされるのを未然防止

SpywareBlaster2.01（フリー）

http://www.javacoolsoftware.com/spywareblaster.html

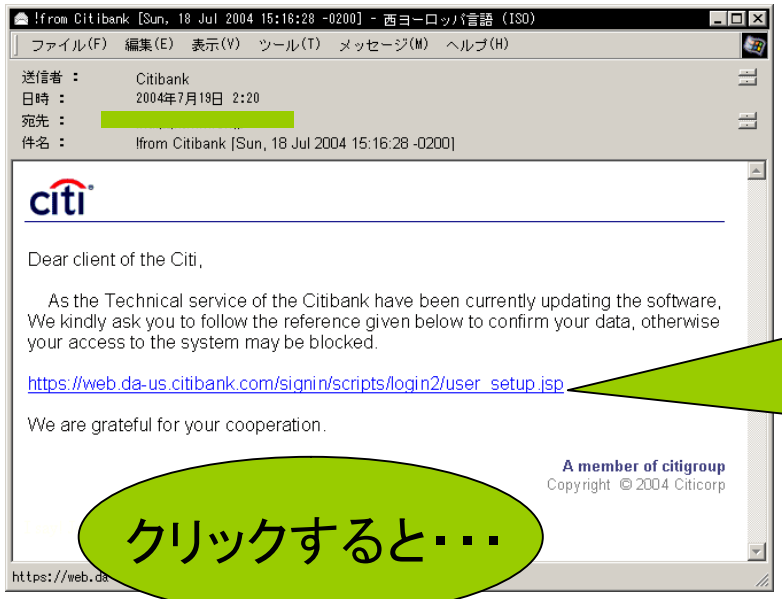
解説：http://www.higaitaisaku.com/spywareblaster.html



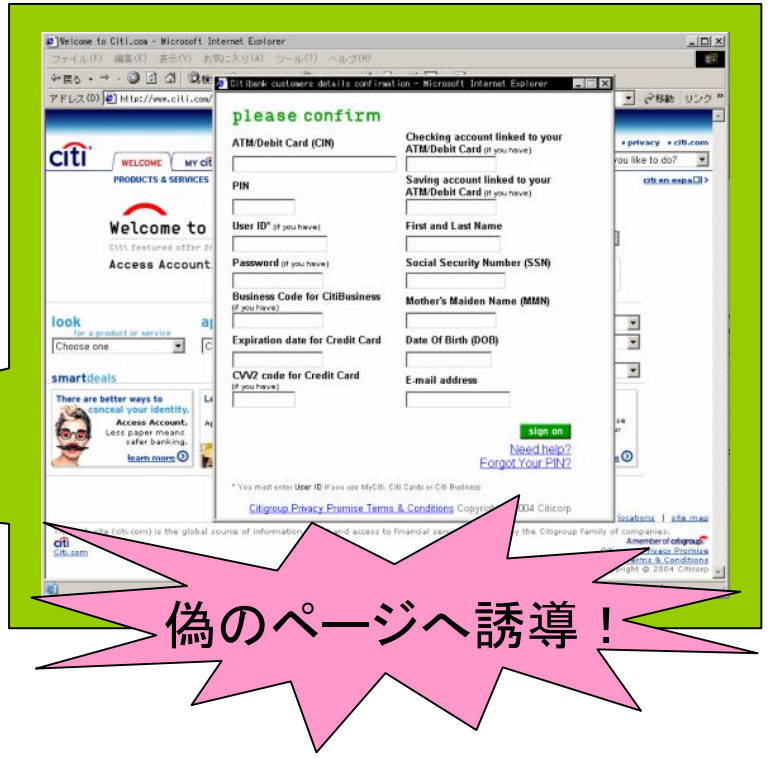
8. フィッシング

ユーザーに偽の電子メールを送りつけ、相手の銀行口座のパスワードやクレジットカード情報などの個人情報をだましとろうとする行為。

一見、CITIバンクからのメール・・・



クリックすると・・・



偽のページへ誘導！

国内フィッシング事案

でもURLがずれてる・・

グーグルツールバーを使用していると正規のURLが欄外に表示されてしまっている

国内フィッシング事案

■平成16年6月 「PSXが当たりました」という偽のソニーからの携帯メールが送信され、偽の発送依頼ページが開設されていた。

■平成16年11月 「イーバンク銀行からのお知らせ[入金がありました]」というメールが送信され、ログインパスワードや暗証番号など入力する偽のページが開設されていた。今回のフィッシング詐欺メールは実際に入金時に送られるメールと同じ件名が使われていた。

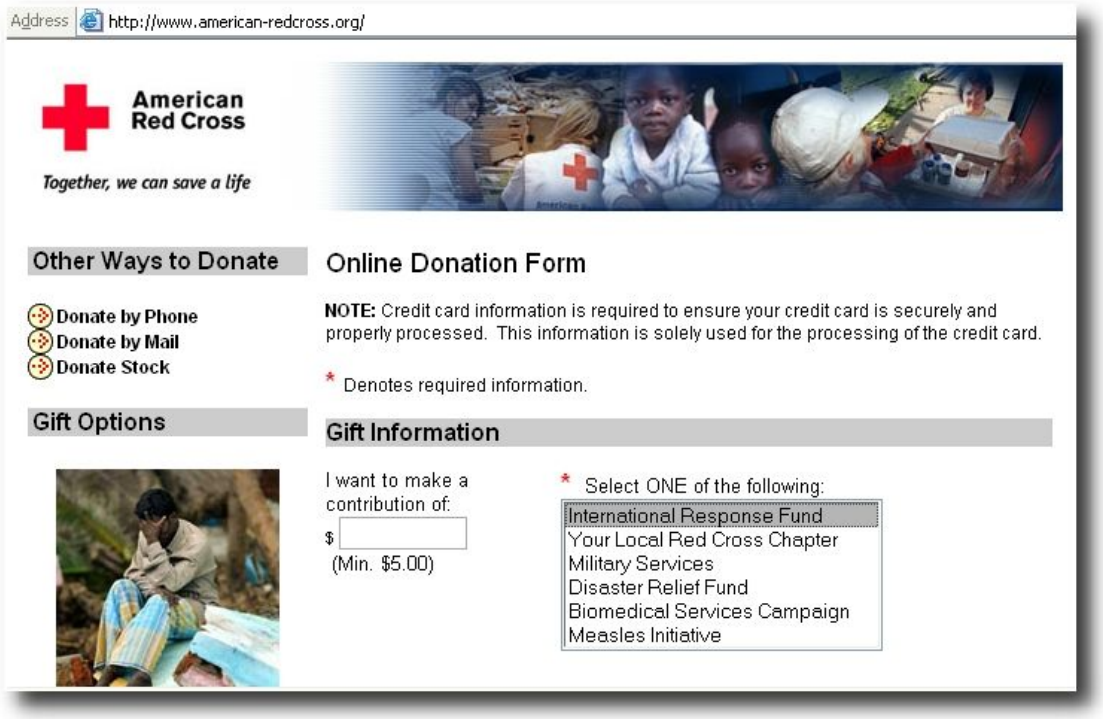
■平成16年11月 「Yahoo!ユーザアカウント継続手続き申請書」というメールが送信され、Yahoo!ウォレットの登録内容を確認変更させる偽ページが開設されていた。I.Eでメールを読んでいる場合、Yahoo!JAPAN IDを抜き出されて画面ごと偽装されてしまう。

■2004年11月「UFJカード」を偽造したメールが送信され、クレジットカード番号などを入力させるページが開設されており、入力した情報を元に作成した偽造カードによるキャッシングで約150万円が不正に引き出されるという国内初の実害発生の事案となった。

海外のフィッシング事案

- 最近は戦争や災害の義援金を名目としたフィッシングが主流

スマトラ沖津波に便乗して詐欺をしかける不正なWebサイトは133にも上った



海外のフィッシング事案

■ハリケーン「カトリーナ」被害に乗じたフィッシング

当時出回ったスパムメールは、ニュース速報を提供する一方で、偽の米赤十字サイトへのリンクをクリックするようメール受信者を誘導した。

このサイトは、Internet Explorerの脆弱性を悪用し、メール受信者のコンピュータにトロイの木馬「Troj/Cgab-A」をはじめとする悪質なコードをインストールしようとする。

一度感染すると、そのPCはハッカーにリモートからコントロールされるようになり、スパイや盗難をしたり、混乱を引き起こしたりするための道具として悪用される可能性がある。

フィッシングのバリエーション

- HOSTSファイルの書き換えによるリダイレクト

- 小規模なファーミング詐欺。電子メールを通じて拡がり、感染した個々のパソコンのローカルホスト・ファイルを書き換えるウイルス――たとえば、主にインターネット・バンキング利用者を狙ったトロイの木馬『バンカー』(Banker)など――を使って行なわれてきた。ホストファイルが書き換えられていると、ユーザーが正しいURLを入力しても、不正なウェブサイトにつながってしまう。

フィッシングのバリエーション

- DNS Poisoningによるリダイレクト=Pharming
- DNSサーバに保存された人気の高いウェブサイトのIPアドレスが、悪質なサイトのアドレスに置き換えられてしまう。このため、正規のウェブサイトにアクセスしようとしたユーザーが偽のサイトへリダイレクトされてしまい、そこで機密性の高い情報の入力を求められたり、有害なソフトウェアをPCへインストールするように指示されることになる。
- 脆弱性を抱えたサーバでは、BINDソフトウェアが安全でない状態で稼働しており、forwarder設定が有効になっているすべてDNSサーバは、BIND 9にアップグレードされなければならない。
- セキュリティ研究者のDan Kaminskyが、250万台のDNSサーバをスキャンしたところ、そのうちの約23万台が「DNSキャッシュ汚染」の脅威に対して脆弱であることがわかった。

偽サイトを見抜く方法

（1）アドレスバーのURLを確認（効果小）

（2）SSL認証発行先の確認（効果中）

（3）フォームの送信先の確認（効果大）

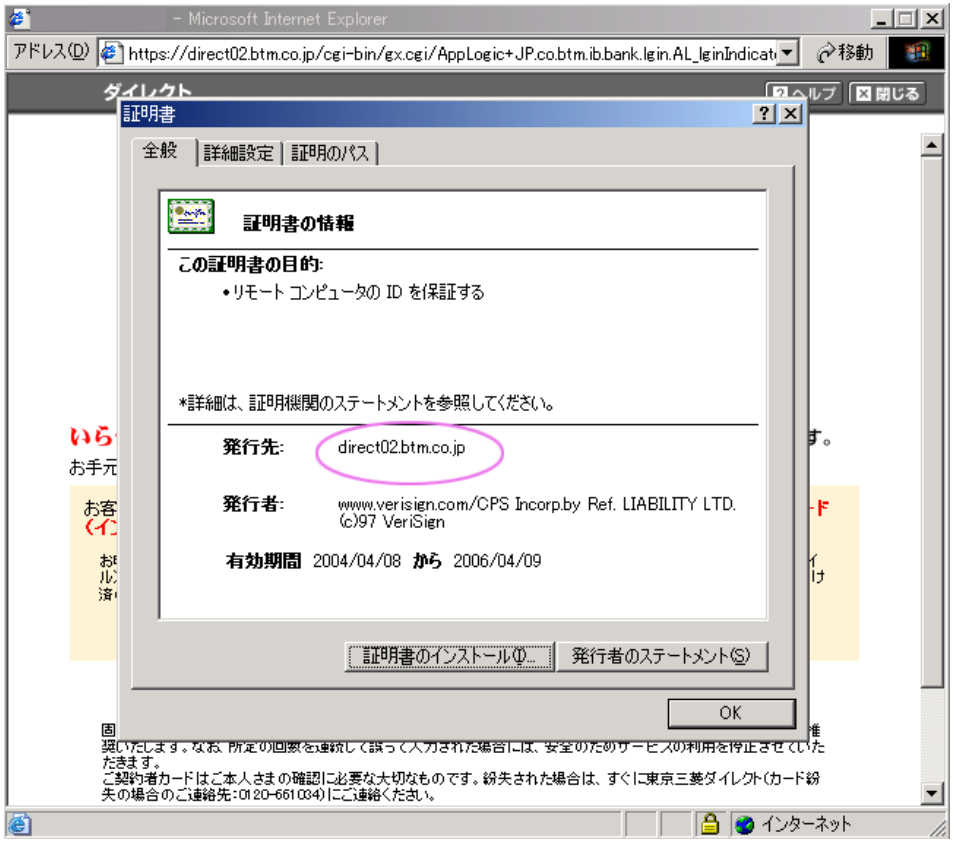
（2）SSL認証発行先の確認

（windowsの場合）

画面右下の鍵のアイコンをダブルクリックして、表示される認証発行先のドメインを確認

（Macintoshの場合）

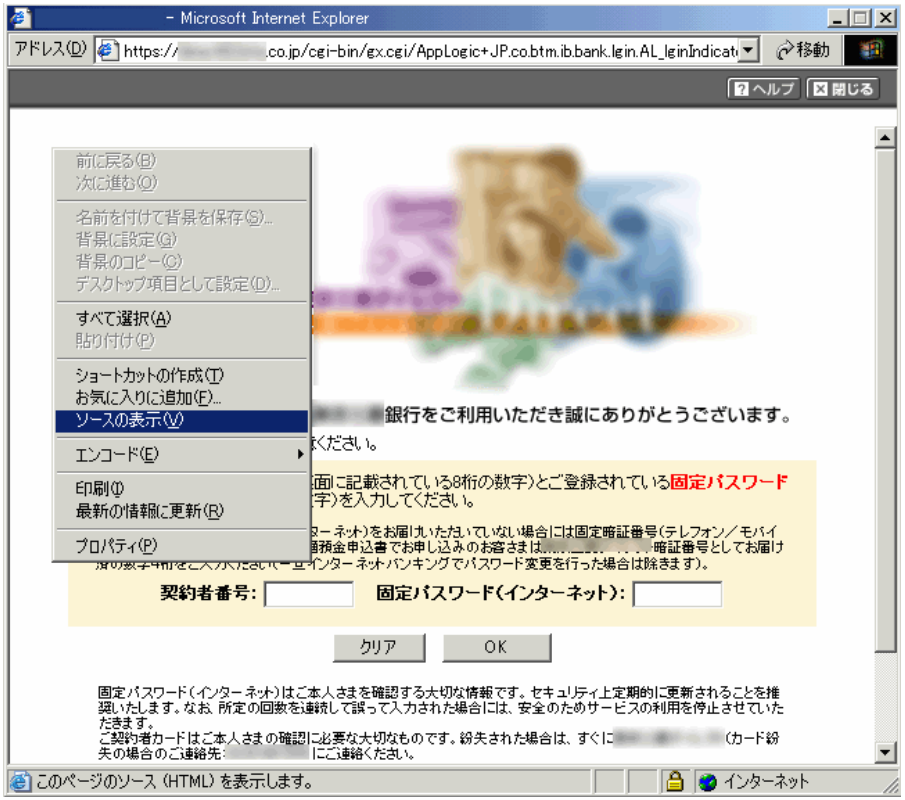
はじめからステータスバーに発行先ドメインが表示されている



Knight of Justice
web110
http://www.web110.com/

（3）フォームの送信先の確認

①右クリックでソースを表示してみる



(3)フォームの送信先の確認

②<FORM ACTION="URL">のURLを確認

AppLogic+JP.co.btm.ib.bank.lgin[1] - メモ帳
ファイル(F) 編集(E) 書式(O) ヘルプ(H)

```
        gintSubmitFlg = 1;
        document.FRM_lginInputId.submit();
      }
    }
  }
}
function autoFocus(){
  document.FRM_lginInputId.TXT_CLIENTIDNUMBER.focus();
}
//-->
</SCRIPT>
</HEAD>

<BODY BGCOLOR="#FFFFFF" onLoad="javascript:autoFocus()">
<FORM NAME="FRM_DUMMY"><INPUT TYPE="HIDDEN" NAME="" VALUE=""></INPUT></FORM>
<FORM NAME="FRM_lginInputId" ACTION="https://direct.btm.co.jp/cgi-bin/gx.cgi/AppLogic+JP.co.
<DIV ALIGN="CENTER">
<TABLE BORDER="0" CELLPADDING="0" CELLSPACING="0" WIDTH="95%">
<TR><TD ALIGN="CENTER">

<DIV ALIGN="CENTER"><IMG SRC="https://www.btm.co.jp/ib/STANDARD/image/login3.gif"></DIV>

<TABLE BORDER="0" CELLPADDING="0" CELLSPACING="5" WIDTH="550">
<TR>

 <TD VALIGN="TOP">
```

フィッシング詐欺対策ツールバー

セキュアブレイン の「PhishWall」（無償）

ブラウザのプラグインとして動作する。アクセスしたサイトごとに正式なドメイン名、IPアドレス、IPアドレスが割り当てられている国名を表示する。想定外の国名が表 示された場合は，フィッシング・サイトの可能性がある。

http://www.securebrain.co.jp/download/index.html

シンセキュアの「SecureVM for AntiPhishing」（無償）

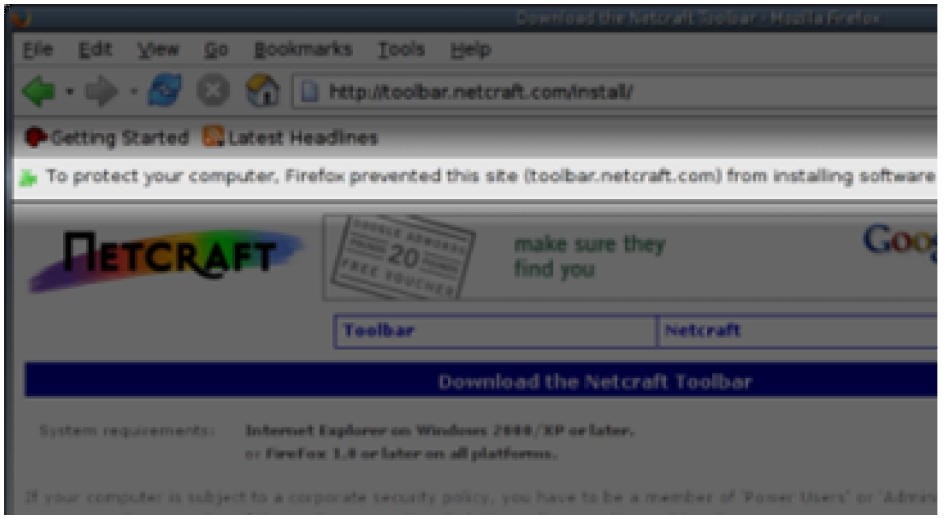
Webアクセス前にあらかじめ起動しておく。するとブラウザのやりとりを監視し、ブラウザがフィッシング・サイトにアクセスすると警告メッセージを出す。

http://www.synsecure.co.jp/japan/antiphishing/download.html

フィッシング詐欺対策ツールバー

フィッシング詐欺サイト データベースに登録済みのサイトやページにアクセスすると、ウェブサイトのホストが実際に置かれている物理的な場所を表示し、疑わしいサイトにいる場合は警告するポップアップを表示する。
また、ポップアップウインドウで故意に隠すことが多い標準のツールバーやアドレスバーなどを強制的に表示する機能や、見誤らせる文字を含む疑わしい URL をトラップする機能も備える。

NetCraft Toolbar
http://news.netcraft.com/



Knight of Justice
web110
http://www.web110.com/

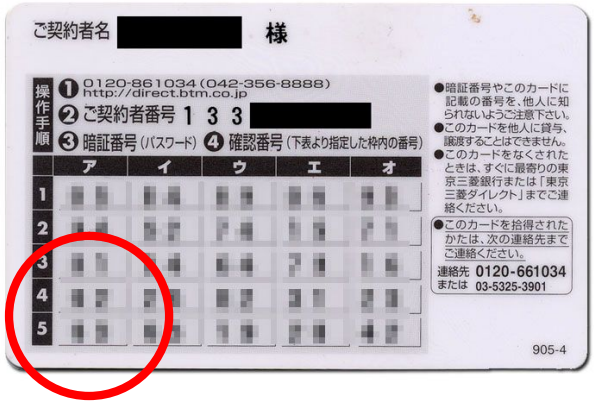
９．ネットバンキング

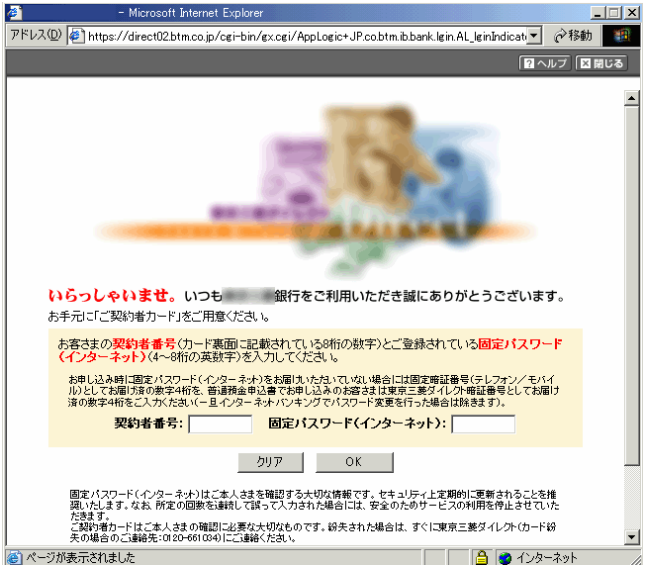
（検挙事例）

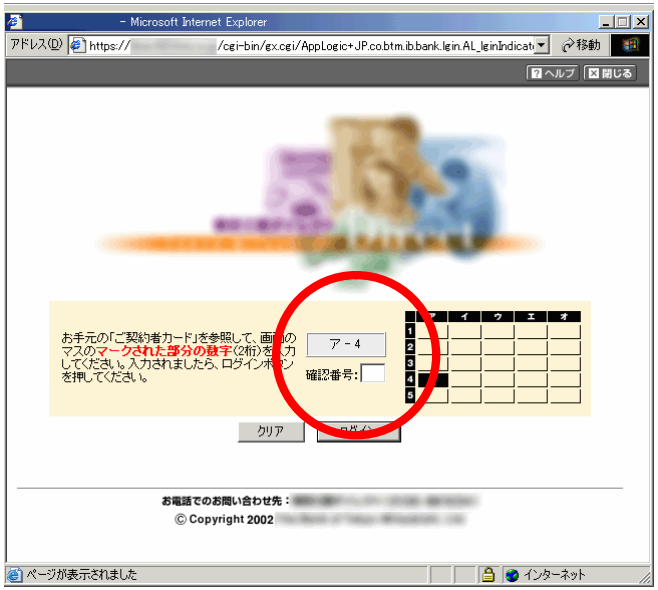
2002年9月、キーロガーで収集した5人のIDでネットバンキングのサーバーに不正アクセスし、そのうちの1人の口座から約1,650万円を自分の口座に送金した無職者ら2人を、不正アクセス禁止法違反、電子計算機使用詐欺罪、組織的犯罪処罰法違反などで2003年3月までに逮捕。（警視庁）

安全なネットバンキングとは？

●乱数表による本人認証







Knight of Justice
WEB110
http://www.web110.com/

万一の被害を最小限に抑えるには

●振り込み限度額を必要最小限に設定しておく

●必要以上の預金を残しておかない

主要ネットバンキングの認証方法比較表

（平成１７年２月WEB110調べ）

http://web110.com/cyberacademy/netbank.html