e-ビジネス情報技術
第8回
情報セキュリティ

講師：片岡　信弘

教科書第10章

ポイント

- 安全なネットショッピングのための行動
- 安全なネットオークションのための行動
- パスワードの適切な管理
- e−ビジネスで守るべきもの
- 情報漏えいの危険性と行うべき対策

10.1 安全なe-ビジネス利用

ネットを日々利用するに当たりなに
に気をつけないといけないか

(1)安全なネットショッピングの利用方法

- Webサイトの確認
  - URLを良く確かめる
  - URLが1文字だけ異なる詐欺サイトなどもあり得る
- 取引の実績
  - 過去の取引実績や利用者の評価などの確認
- 相手の確認
  - 取引相手氏名，住所，電話番号など確認
- 取引条件
  - 商品返品や交換可否，代金支払方法など利用規約確認
- 個人情報の取り扱いの確認
  - 「プライバシーについて」，「個人情報について」など個人情報の取り扱いの考えを確認

- オリンピック　https://id.tokyo2020.org/

オークションサイトでの特別な注意事項

- オークションは思わぬところに誘惑が存在する
- 楽天オークションサイトでは次のような注意を喚起
  - 市場価格から桁外れに安い，入手困難なもの，うまい話しは，注意が必要
    - もっと安く譲るからメールアドレスを教えて
    - オークションを介さずに直接取引をしましょう
  - など，巧みに近づいてくる直接取引や個人情報開示の勧誘には，思わぬトラブルに巻込まれてしまうおそれがある
  - 自分の取引相手として相応しい相手か見極めることも重要です

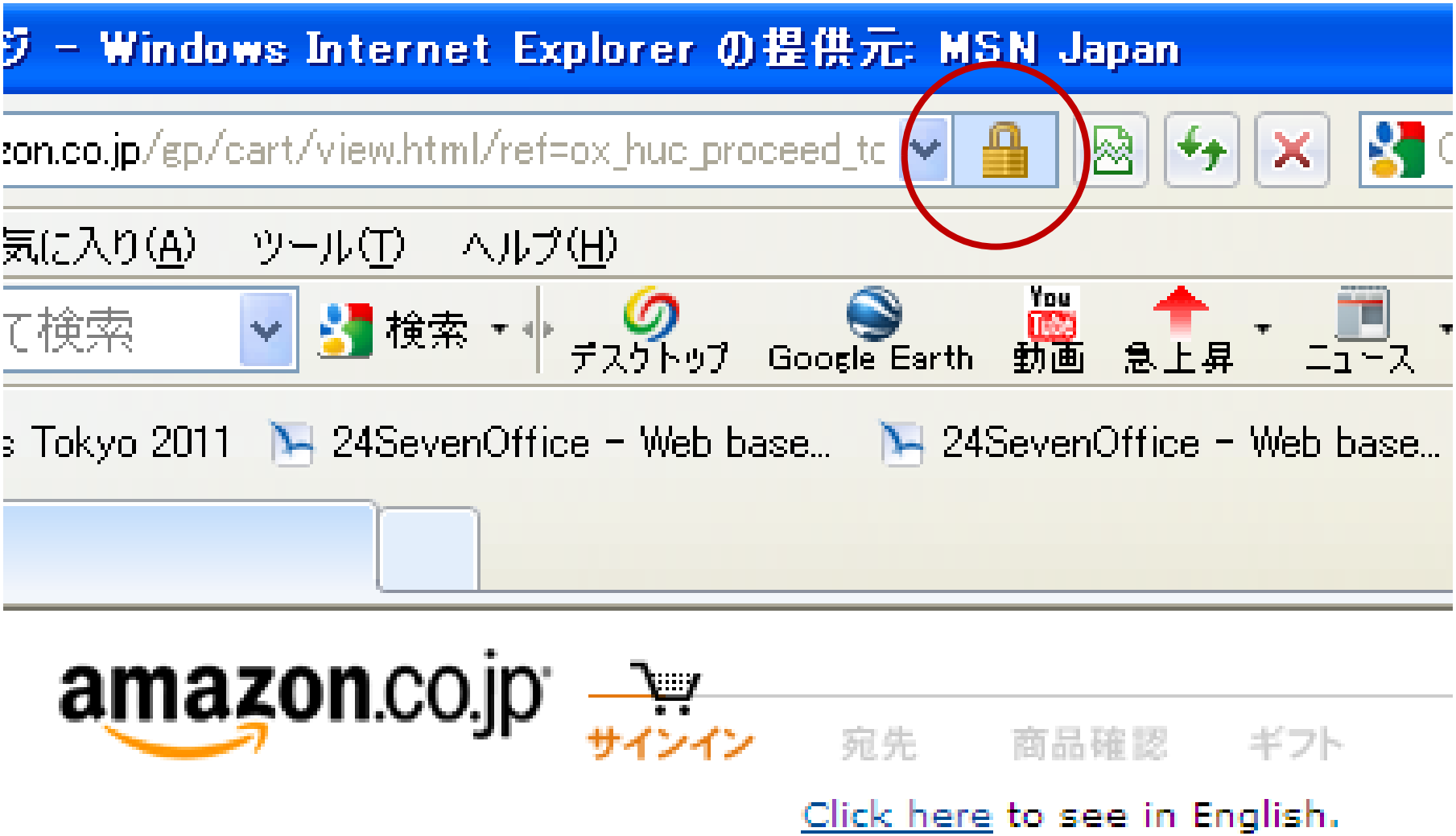
(2) フィッシング詐欺

- フィッシング詐欺
  - 巧みにユーザIDやパスワードを盗み出す行為
- いつも使っている「銀行と思われる差出人」から「〇〇銀行より緊急のご連絡」
  - お客様の口座で不審な取引が確認されています．今すぐに下記のリンクにアクセスして、お客様の口座情報を確認してください．
  - システム変更に伴う本人確認のため口座番号，パスワードを入力してください
  - パスワードが無効となりました口座番号，パスワードを入力してください
- フィッシングサイトに誘導され．このサイトで口座番号，パスワードを入力すると情報はすべて盗取される

フィッシング詐欺にかからないために

- 銀行からはこのようなメールは，絶対に発信さないことを認識する
- 巧妙に作成されたフィッシングメールやフィッシングサイトを正確に見抜くことは意外と困難
- 安全だと確証ないサイトでは，情報を入力しないことが最善
- Web サイトの安全確認としては，ドメイン名を確かめること
- 入力時Web ブラウザ左上に鍵マークがあることの確認
  - 鍵マークは認証された正規のサイトの意味する
  - SSL と呼ばれる暗号化通信の仕組みを利用
    （Secure Sockets Layer ）
- これらはPC、スマホも同じ
- 事例紹介　https://www.sagiwall.jp/education/virtual.html

図10.1 鍵マークのあるWeb入力サイト



偽通販サイトに注意

- 本物そっくりの偽通販サイト/偽もの販売するサイト
  - 検索エンジンでたまたまヒットしたサイトは危険
  - 一定の有名どころを利用する
  - 価格.comなどの比較サイトを利用する
- 怪しさのチェツク
  - 連絡先がフリーメー
  - 代金の支払が銀行振り込みしか無い
  - 会社名義でなく個人名義
  - ログイン等のときWebサイトに鍵マーク表示がない
  - 極端な値引き

ネットバンキングの詐欺被害額(番外)

- 被害額推移(注1)
  - 2017年：約11億円
  - 2016年：約17億円
  - 2015年：約31億円
- 個人よりも法人の被害額が増加
- 個人顧客の場合は基本的には被害は補償される
  - ただし重大な過失があれば不可
  - 重大な過失とは　　Quiz1

(注1)広報資料　平成30年3 月22日　警察庁より

(3)悪意のあるサイトでの被害に対する注意

- 悪意のあるサイトとは
  - ◆閲覧によりウイルスに感染する攻撃サイト
- ウイルス対策と共にWebブラウザ対策が必要
  - ◆悪意のあるサイトはJavaScriptをWebページに埋め込み情報やファイルを盗取
  - ◆信頼あるサイト以外ではJavaScript実行させない

- **JavaScriptの無効化設定方法**

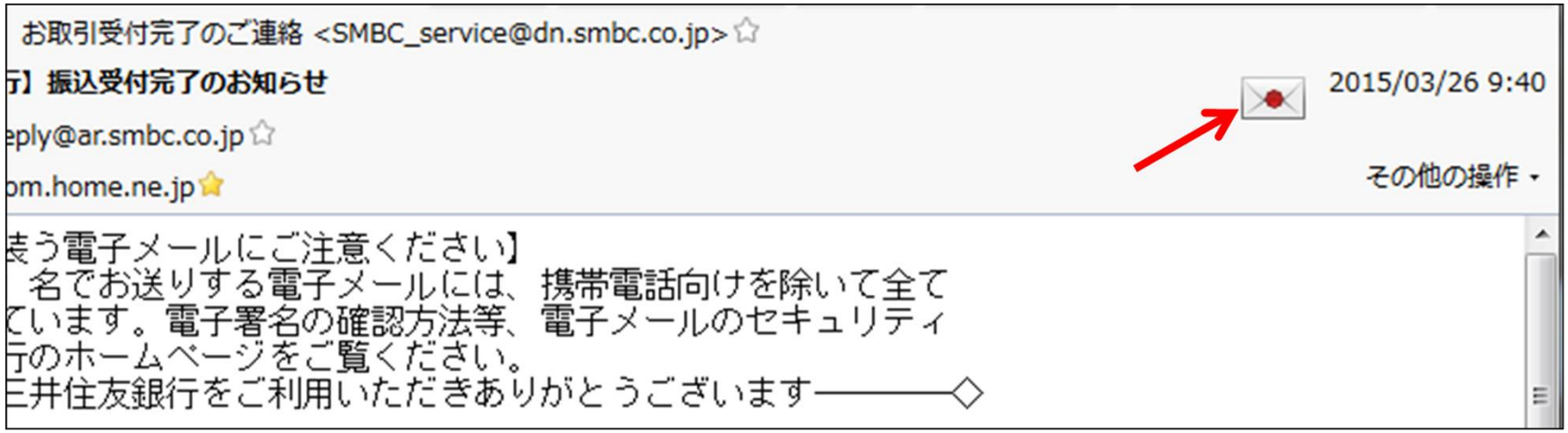
http://www.netyasun.com/browser/javascript.html

(4)ワンクリック詐欺にあわないために

- 電子メールを送りつけ記載されているサイトをクリックすると脅迫めいた文面，手口で料金の振り込みを迫る
- 怪しげな電子メールに記載されたサイトは，クリックしないことが原則
- クリックしても契約成立しないので料金請求には何ら法的拘束力はない
- 事例 http://urx.blue/teWB

(5)メールの信頼性

- 銀行等から発信されるメールは電子証明書が付いてきます
  - Web メールはこの機能に対応していない
- スマホで電子署名の機能をサポートしいるものはない.
  - 正当性は，誰が送付してきたかを確認するのが良い
  - 発信人は画面に表示されないので，転送指定により元のメールと共に送信元のアドレスを表示する



(6)サポート詐欺

- ウイルスに感染しているといてサポート費用を要求する詐欺

10.2 パスワードの適切な設定と管理

パスワードを適切に管理し
被害に会わないようにする

パスワードが盗取された時の被害

- 通常銀行ネットバンキングは暗証番号と暗証番号表⇒ワンタイムパスワードを利用
- ネット専用銀行はユーザIDと複数のパスワードのみ
  - 通常使用と異なるパソコンからアクセスを行った場合ユーザIDとパスワード以外に合言葉を要求
- ネットオークションでは他人のユーザIDとパスワードによる不正な出品登録や落札の可能性
- ゲームサイトでは他人のポイントの不正な利用
- メールが他人に読まれることにより，個人情報が漏えいする危険性が存在

ワンタイムパスワード事例

安全なパスワードの設定

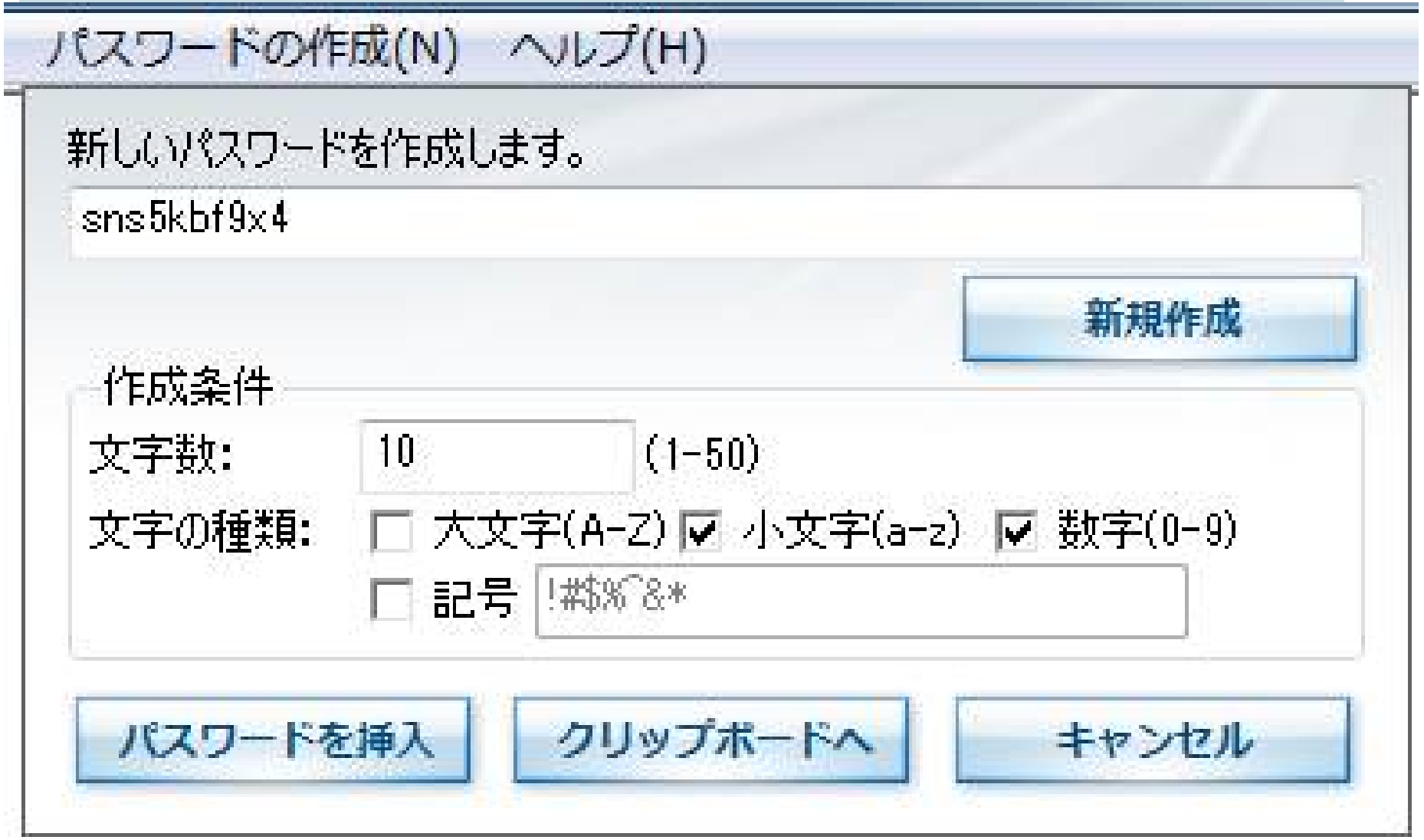
- 個人情報からは推測できないこと(ダメ事例)
  - asano　nakayama　fujiwara（名前）
  - 19691104　s640108（生年月日）
  - john　ranran　kenken　（ペットの名前）
- 英単語をそのまま使用しないこと(ダメ事例)
  - microsoft　dialog　monkey
- 適切な長さの文字列であること(ダメ事例)
  - ps　ks　nk
- 類推しやすもの安易な組み合わせでない
  - abcdef　12345（安易な数字や英文字の並び）
  - qwert　asdfgh（キーボードの配列）

- アイドルのブログが荒らされたの被害はなぜ起こる Q2

パスワード作成ソフト

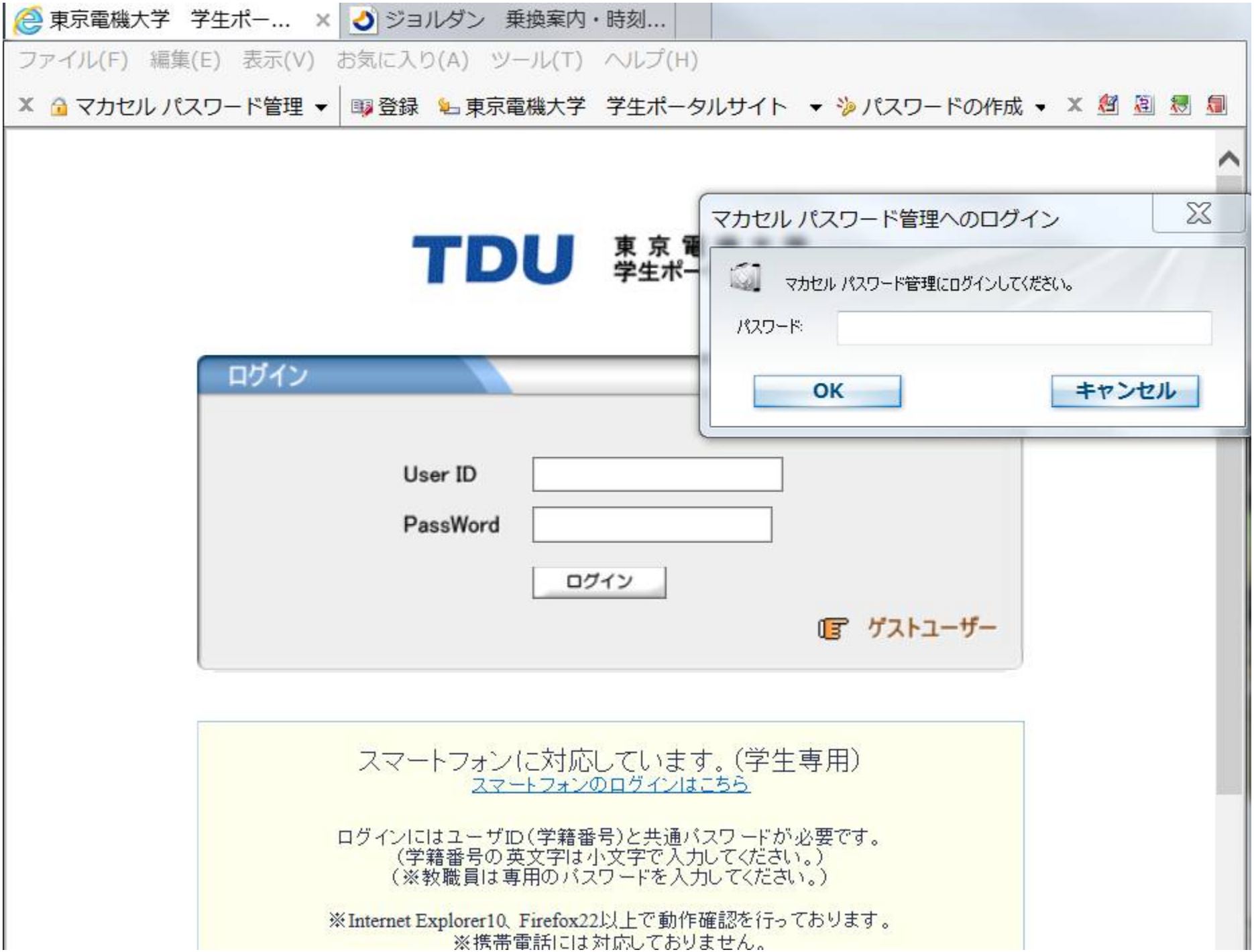
- パスワードの要件
  - 8文字以上の一定の長さを持つ
  - 英字，数字の組み合であること
- パスワードを作成するのは意外と困難
- パスワード生成ソフトウェアの利用
  - 以下の条件でパスワードをランダム生成
    - 使用する文字種(数字，大文字，小文字など)
    - パスワード桁数

マカセルパスワード管理-パスワード生成



パスワードの安全な管理

- パスワード管理の注意項目
  - パスワードは他人には教えない
  - パスワードをそのままパソコン内で管理しない
  - ユーザ名やパスワードを電子メールで送付しない
  - パスワードを他人に読まれないように注意する
  - パスワードを書いたメモをしまう時は鍵をかける
  - パスワードの使い回しをしない
  - パスワードを定期的に変える⇒?.
- 多数のパスワードの定期的な変更は面倒
  - パスワード自動管理ソフトの利用


東京電機大学　学生ポー...
ジョルダン　乗換案内・時刻...
ファイル(F)　編集(E)　表示(V)　お気に入り(A)　ツール(T)　ヘルプ(H)
マカセル パスワード管理
登録
東京電機大学　学生ポータルサイト
パスワードの作成
TDU
東京電
学生ポー
マカセル パスワード管理へのログイン
マカセル パスワード管理にログインしてください。
パスワード:
OK
キャンセル
ログイン
User ID
PassWord
ログイン
ゲストユーザー
スマートフォンに対応しています。(学生専用)
スマートフォンのログインはこちら
ログインにはユーザID(学籍番号)と共通パスワードが必要です。
(学籍番号の英文字は小文字で入力してください。)
(※教職員は専用のパスワードを入力してください。)
※Internet Explorer10、Firefox22以上で動作確認を行っております。
※携帯電話には対応しておりません。

10.3. インターネットビジネスで何を守るか

セキュティの脅威に対して，インターネットビジネスで守るべきものは何か

e-ビジネスを行う企業側

- ビジネスを行っていくための各種の**企業の戦略情報や経営**のための情報
  - 新しいサービスをいつから開始するといった情報はタイミング良く発表が必要
- 顧客の**個人情報**
  - 個人情報の漏えいは，その企業の信用を傷つけ，ビジネスに大きな打撃を与える
- インターネットビジネスを行うための**サーバ**そのもの
  - Webサイトが改ざん，ウイルス感染によるファイルの流出/破壊を防ぐことが必要

e-ビシネスを利用する個人

- IDやパスワード
  - クレジットカード番号，ネットバンキングのユーザIDやパスードなどの盗取で大きな損害を被る
- パソコン内の情報
  - 個人のパソコン内の自分/他人個人情報流出で損害を被る
- 個人のWebサイトの書き換えの被害にも注意
  - 情報セキュリティ対策の甘い個人のWebサイトを無差別な攻撃も存在

踏み台にされないこと

- 踏み台とは
  - 自分が気づかないうちに管理者権限のユーザIDやパスワードを盗取されパソコンを自由に操作できる状態にされること
- 不正アクセスや迷惑メール配信の**中継地点**に利用される
- 踏み台とされたパソコン持ち主が不正行為を働いているように見せかけられる
- パソコン所有者はインターネット上での**信頼を失い**，**犯罪関与**の疑がわれ，警察による**逮捕もあり得る**

10.4. 情報漏えいのパターンと事例

企業からの情報漏洩は，不正アクセスや不正プログラムによるものよりは，基本的な過ちや内部犯行の割合の方が多い

図10.4 情報漏えいの原因割合

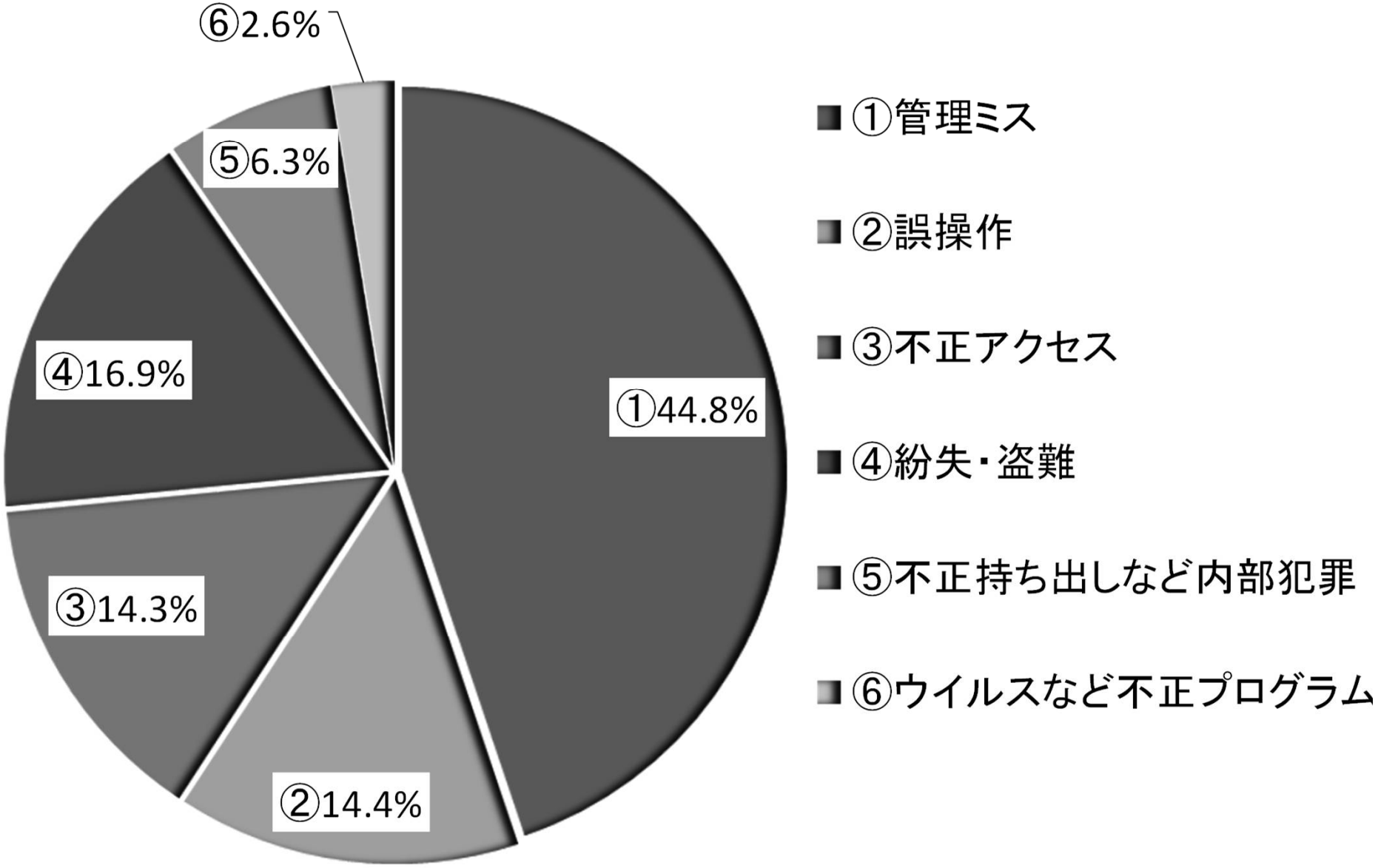
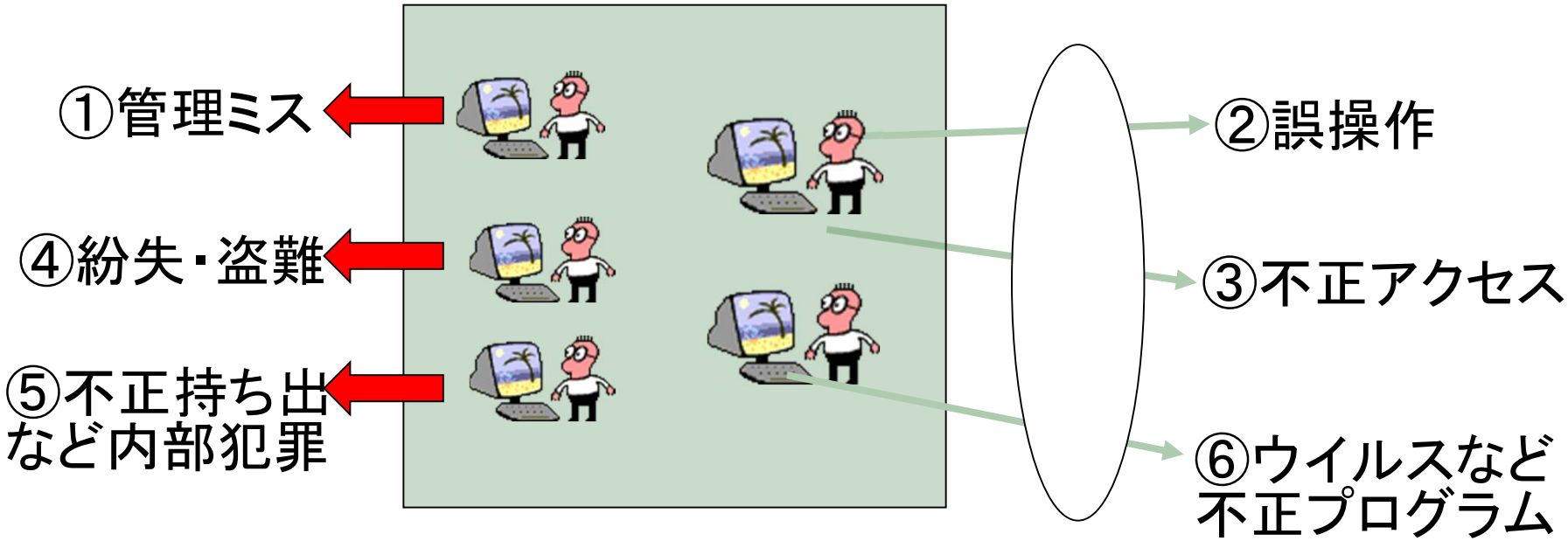


図10.5 情報漏えいのバターン



情報漏洩の原因

- 1.管理ミス
  - 引越しの際の誤廃棄，個人情報の受け渡しミスで個人情報が紛失
- 2.誤操作
  - 多数の人にメールを発信する時，TO やCC で宛先を指定
  - 顧客名簿などをWeb 上で外部から見えるディレクトリ設定
- 3.不正アクセス
  - 不正に手に入れたユーザID，パスワードで外部からのインターネット経由での不正なファイルアクセス
- 4.紛失・盗難
  - パソコンの盗難や紛失
  - 重要な情報は暗号化しておく
    - Word/EXCEL:ホーム⇒情報⇒文書の保護

情報漏洩の原因その2

- 5.不正持ち出しなど内部犯罪
  - 社内の人間の情報の意図的な持ち出
  - USB などの外部記憶装利用，メールの添付で情報を外部に送信
- 6.ウイルスなど不正プログラム
  - ウイルスなど不正プログラムによる情報流出
    - 確実なウイルス対策が必要
    - 利用ソフトを常に最新にする

表10.1　情報の漏えい事例　部分

企業名	情報内容	発表/発覚時期	漏えい規模	原因
Yahoo! BB	氏名などの会員情報	03年9月	451万件	恐喝による管理者ID，パスワード入手
KDDI	顧客契約情報	06年6月	399万件	内部人為的なもの
大日本印刷	DMのための個人情報	07年3月	863万件	委託先社員の　不正持ち出し
モンベル	クレジットカード情報	10年3月	1万1千件	SQLインジェクション
ベネッセ	ゼミなどの登録者情報	14年7月	760万件	委託先社員の　不正持ち出し
イプサ	個人情報	16年11月	48万件	不正アクセス

クッキー(Cookie)に対する認識

- クッキーはそれぞれのユーザに対応したデータを保持しておき次からはこれを利用し各ユーザに必要なWebページを表示させる
- ロクイン/ログアウトもクッキーを利用
  - 一度ログインするとログアウトするまで，ログイン状態を保持
  - 保持しているクッキーをやり取りし状態を持続
  - ログアウトの時はクッキーを削除
- サイトによってはアクセスを行うと自動的にログイン状態となり「こんにちは，片岡さん」と表示
- クッキーを削除せずそのまま利用しているケース
- 便利ではあるがクッキー情報が盗取される危険性があることを認識する必要あり

クッキーによるアクセス追跡

- ネットショッピングサイトでユーザがどのようなサイトを閲覧したアクセス追跡のめにクッキーを利用
- 楽天でのクッキーの利用に関する表示
  - 当グループでは下記の行動ターゲティング広告を行っています.
  - 行動ターゲティング広告とはサイト閲覧情報などをもとに来訪者の興味・関心にあわせて広告を配信する広告手法です
  - 当広告の無効化をご希望される方は、お手数ですが以下の手順に従いクッキーを無効化ください

    http://grp01.ias.rakuten.co.jp/optout/

関連サイト

- 第1回：PC内部のファイルを人質にとるランサムウエア「CryptoWall」
  - http://itpro.nikkeibp.co.jp/atclact/active/15/030500023/030500001/?act05
- 第2回:日本のインターネットバンキングを狙う詐欺ツール「AIBATOOK」
  - http://itpro.nikkeibp.co.jp/atclact/active/15/030500023/030500002/?act05
- 第3回：巧妙な隠蔽技法を備えた標的型攻撃用ツール「BKDR_PLUGX」
  - http://itpro.nikkeibp.co.jp/atclact/active/15/030500023/030500003/?act05

10.5 ファイル共有ソフトウェアによる情報漏えいの危険性

ファイル共有ソフトにより企業や官庁の重要な情報や学校の生徒の成績等の個人情報が漏えいする事件が多発

危険性と不法性について説明する

ファイル共有ソフトウェアの危険性

- WinnyやShareのファイル共有ソフトウェアとは
  - 匿名でファイルの公開と流通を効率よく行うことが目的
  - どのようなファイルを持っているかの情報をキーとしてネットワーク上に配布
  - 他コンピュータはそのキーを元に必要なファイルの入手
- ファイルは暗号化されるためウイルスチェックにかかりにくく，ウイルスに感染したファイルが取り込まれる可能性が大
  - ウイルスに感染すると今度は，ファイル共有を想定していないファイルまでウイルスにより流出する
- ワクチンソフトを設定しているからといって安全ではない
- ファイル共有ソフトウェアで入手する音楽などのファイルは著作権上の問題も多く，この面からも利用は原則禁止

表10.2 ファイル共有ソフトウェアによる情報流出事例

組織名	発生年月	プログラム名	事　象
山形県警	2007年2月	Winny	巡査長の私物パソコンから犯罪被害者など約610件の個人情報を含む捜査情報が流出
三井生命	2007年3月	Winny	業務契約先社員の私物パソコンから過去に持ち出した企業年金の顧客など1501人分の個人情報が流出
春日部市	2007年3月	Share	職員自宅の私物パソコンから国民健康保険加入者情報約5000人分と，個人事業者の個人情報約6000人分が流出

日経コンピュータ　2007年5月14日号 pp123　より

まとめ

- 利用するWebサイトのURLは良く確かめる
- ネットオークションの相手はよく確かめる
- ネット詐欺に遭わないように気を付ける
  - ワンクリック詐欺、サポート詐欺、フィッシング詐欺
- パスワードの適切な管理をする
  - 複雑なものとする
  - 使い回しをしない
  - 管理を確実にする
- 情報漏えいの危険性と行うべき対策
  - パソコンの持ち歩きの注意
  - メール宛先の注意
  - 確実なウイルス対策
  - 利用ソフトを常に最新にする
  - 重要な情報の暗号化