IPA
Information-technology Promotion Agency, Japan

初めての情報セキュリティ対策

IPA 技術本部セキュリティセンター

新入社員の皆さん
「情報セキュリティ対策」って
ご存知ですか？

リテラシー

- リテラシーとは元々「言語により読み書きできる能力」をさす言葉でしたが、最近では、自分が身につけた知識や技術を使って、事象を理解・整理し活用する能力のことを指すようです
  - 情報リテラシー
  - コンピュータ リテラシー

セキュリティ対策：技術的対策

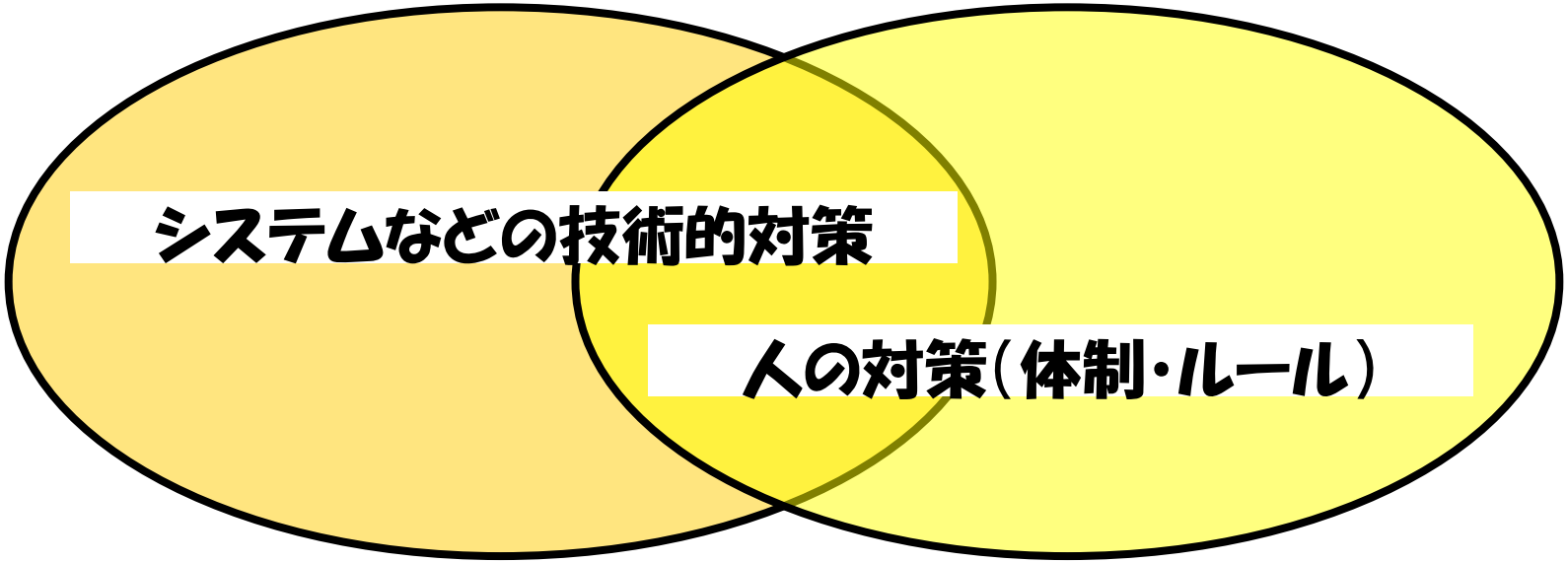
- 自分のコンピュータを守ること・・・
  - コンピュータウイルス対策
  - 脆弱性の解消
  - 情報の暗号化
  - 情報のバックアップ
- 企業内ネットワークで言えば・・・
  - ファイアウォール
  - IDS（侵入検知システム）/IPS（侵入防止システム）
  - プロキシサーバにおけるネットワーク監視・制御

セキュリティ対策の変化

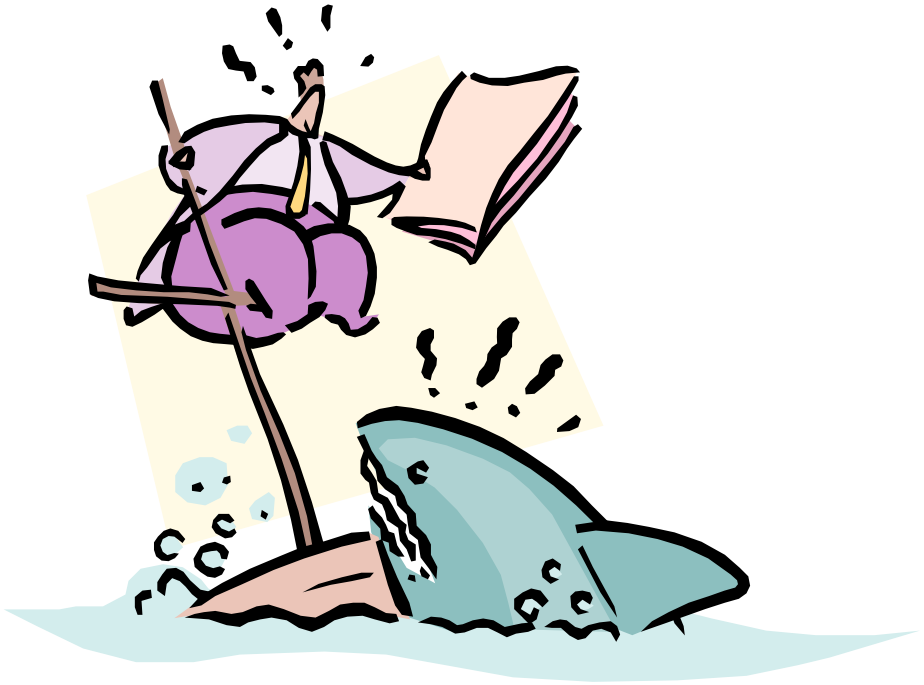
- 個人情報保護法の施行に伴い、**個人情報の漏えい問題**が大きく取り沙汰されるようになっています
- 個人情報や企業における企業情報や機密情報を守ることが重要なポイントとなってきました
- 企業で取り扱う情報を守るためには、それらの情報を管理するためのコンピュータやネットワークの技術的なセキュリティ対策も当然必要ですが、それだけではなく、「**人のセキュリティ対策**」も重要になってきました

人のセキュリティ対策

- 「人のセキュリティ対策」とは、いわゆるセキュリティ対策ルールや体制を決め、それを守ることです



情報セキュリティ対策



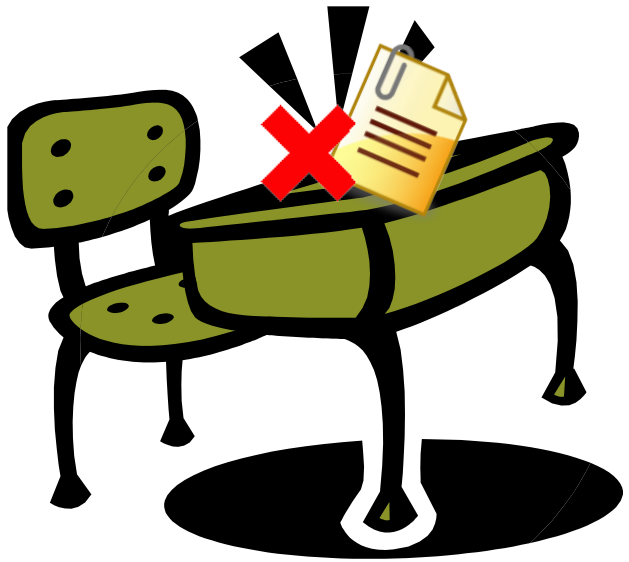
対策1：企業にとって重要な情報って・・・

- 企業にとってその情報が企業外に漏れると、企業の事業運営上で重大な問題を引き起こす可能性のある情報が重要な情報です
  - **お客様から預かっている個人情報**
  - **企業で働く従業者の個人情報**
  - **企業運営のための企業情報**
  - **ノウハウ等の機密情報**

- 何が重要な情報か理解することが情報セキュリティ対策の第一歩と言えます

対策2：事務所の机の上は…

- 机の上に放置した情報は、誰かに持ち去られる危険にさらされています
- 関係者以外が見たり触れたりできないよう、**重要情報は放置せず**、管理および保護する必要があります



パソコン・記憶媒体も・・・

- 机の上に放置した○○は、誰かに持ち去られる危険にさらされています
- 関係者以外が見たり触れたりできないよう、重要○○は放置せず、管理および保護する必要があります
- 特に夜間は・・・

対策3：知らない人が事務所に・・・

- 関係者以外の社内の立ち入りを制限しなければ情報を盗み取られる危険性があります
- 特に重要な情報が格納されたサーバや書庫・金庫などの近くには無許可の人が近づいたり、操作できないように・・・

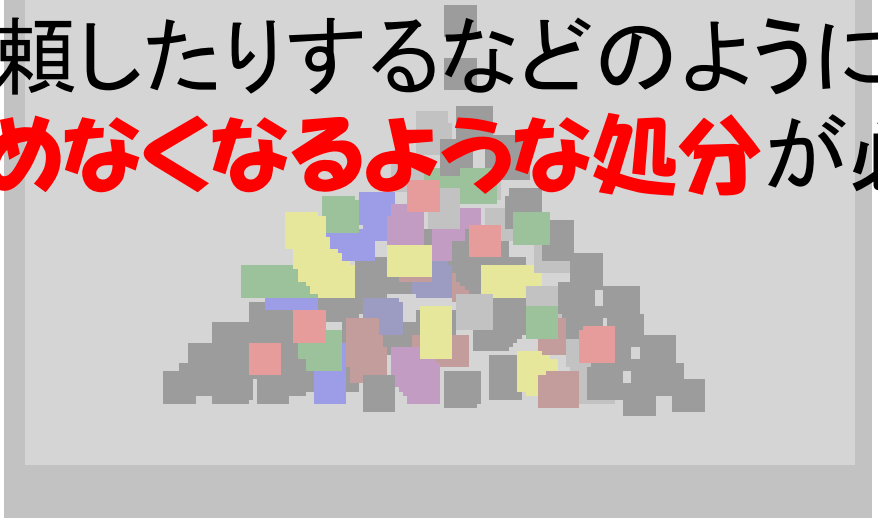
事務所で
見知らぬ人を見かけたら・・・
声をかけるなどのように
無許可の人の立ち入りが
ないように・・・

こんな対策が効果的・・・

- 事務所で見知らぬ人を見かけたら、
  「**誰をお探しですか？**」とか
  「**何か御用ですか？**」
  というような声をかける
  ことが良いでしょう。
  本当に仕事に来ている人
  であれば失礼のないように…
  悪い人であれば大きな牽制に
  なるはずです

対策4：重要な情報の処分は・・・

- 重要な資料などを廃棄する場合は、シュレッダーで裁断するなどのように、**重要情報が読めなくなるような処分**が必要
- 重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼したりするなどのように、**電子データが読めなくなるような処分**が必要

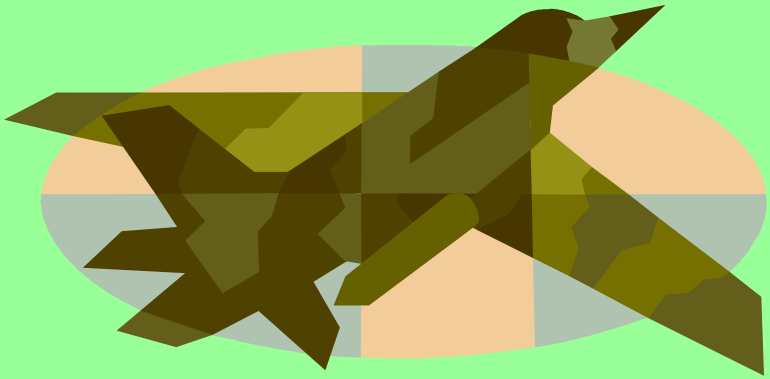


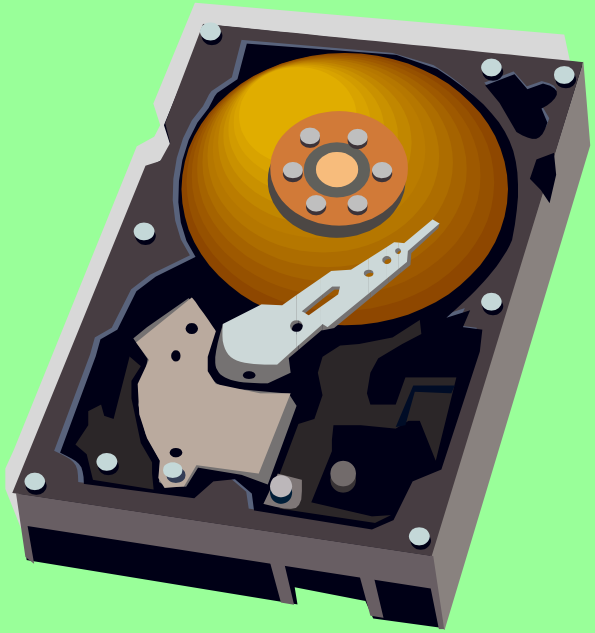
事例：一般家庭ゴミ？

- 会社で終わらない仕事を自宅に持ち帰り、そのときに使用した重要な情報が記載されていた書類を、不要になったので**一般家庭ゴミの回収に出した**。その資料が地方自治体の住民情報だったので、回収業者はビックリして自治体に報告し、大騒ぎになった。情報漏えいはしなかったけれど…

事例：びっくりな事例

- 米国軍需メーカーの機密情報、ガーナで販売されていた中古HDDから発見 廃棄PCから取り出された？ 国防情報局やNASAなどとの契約文書が数万件





ゴミ箱あさりから始まる情報漏えい

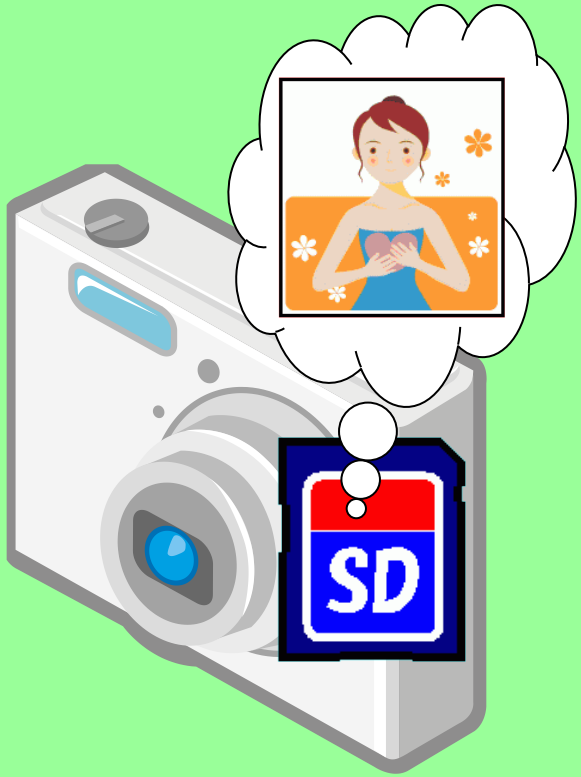
- ソーシャルエンジニアリング(Social Engineering)と呼ばれる情報を奪取する手法では、『ゴミ箱あさり』が有名です
- ある会社から情報を盗み出そうとしている悪者は、まず手始めにその会社のビルのゴミ置き場においてある廃棄書類を物色すると言われています
- ここから、情報漏えいが始まるといっても過言ではありません

廃棄しない場合、こんな事例も…

●友人からデジタルカメラのメモリがいっぱいになったので予備のメモリを譲ってと言われた。そこで、以前利用していた予備のメモリをカメラでフォーマットして友人に譲ったのだが…

●友人から「**お前の彼女綺麗だね**」って言われたけど、確か紹介してないよなぁ？

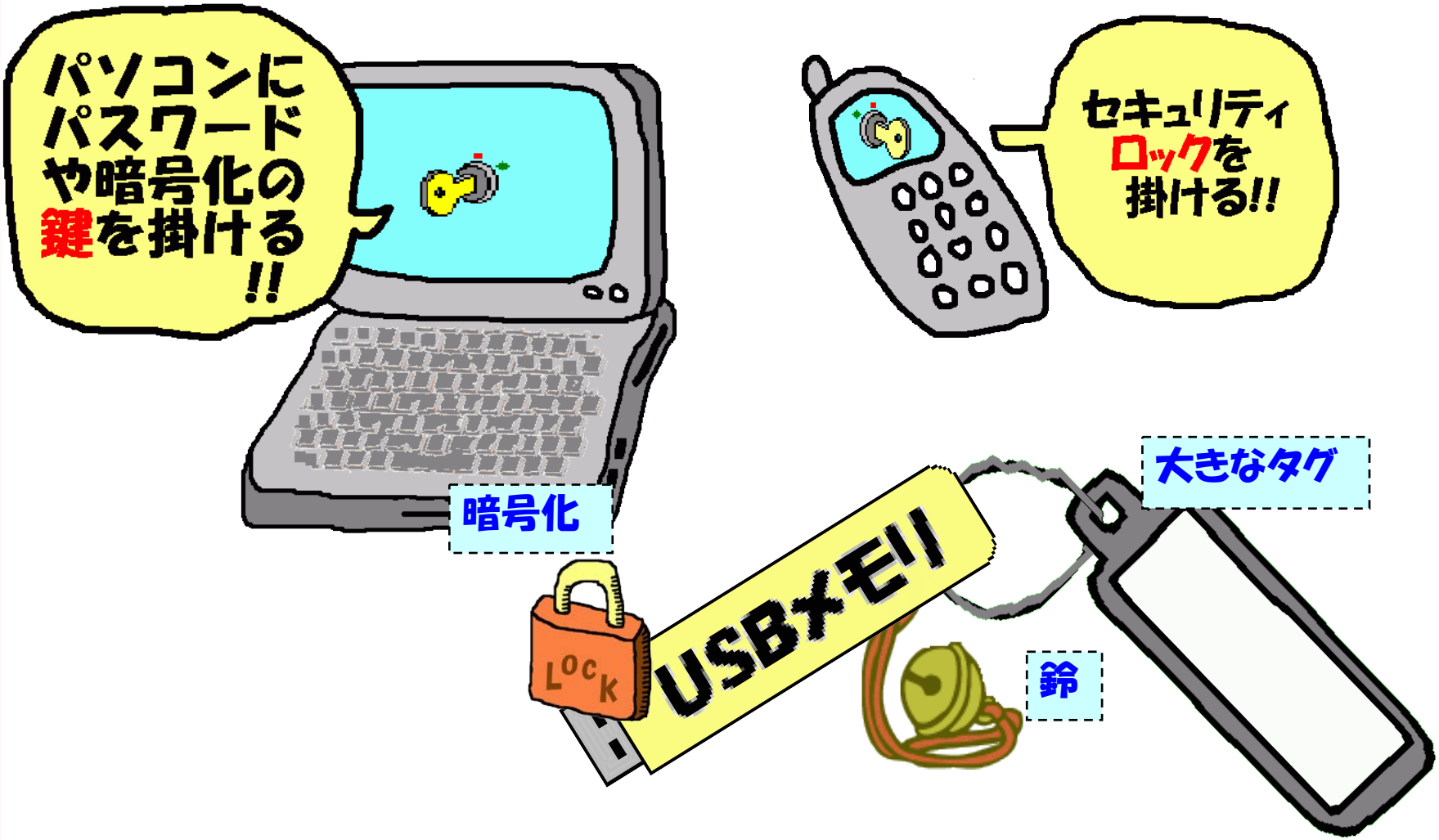
●友人は、譲られたメモリを興味本位から復元ソフトでデータ復元したようで、見せたくなかった写真まで見られてしまいました…



対策5：重要な情報の持ち出し・・・

- 情報の社外への持ち出しにおいては、**「そもそもこの情報は持ち出していいのか」**を確認する必要があります
- 重要な情報を会社の外へ持ち出す場合は、**上司の許可**が必要、さらに**持ち出し記録を残す**必要があります
- 持ち出した情報は、思わぬ盗難にあったり、うっかり紛失したりすることがあります。情報が格納された携帯電話やパソコンやデータファイルにパスワードを設定するなどの対策を事前に行っておけば、盗難・紛失時に情報を簡単に見られないようにすることもできます

持ち出しの物理的な対策



のぞき見から始まる情報漏えい

- ソーシャルエンジニアリング(Social Engineering)と呼ばれる情報を奪取する手法では、『ショルダーハッキング』も有名です
- 最近電車の中などでスマートフォンや携帯電話、さらにはタブレットやパソコン等を利用している人が増えています
- 情報を盗み出そうとしている悪者が、そういった人たちの周りにいるかも知れません

と言うことで・・・

- 不必要な持ち出しはしない
- 持ち出す情報について、上司や管理者の許可を得て、さらに持ち出し記録を残す
- 持ち出す方法(ＣＤ／ＤＶＤ、USBメモリ、パソコン等)について上司や管理者の確認（暗号化やロック、リモート操作等のセキュリティ対策がされているか）を得る
- 重要情報が格納されたスマートフォンやタブレット、パソコンは、第三者の多く集まる場所（電車の中、待合室、喫煙所等）では利用しない
- 書類のまま持ち出す場合はカバンに入れて肌身離さず持ち歩く（間違っても電車の網棚に放置しない等）
- 持ち出し先で安易に捨てない（廃棄しない）

対策6：パソコンは・・・

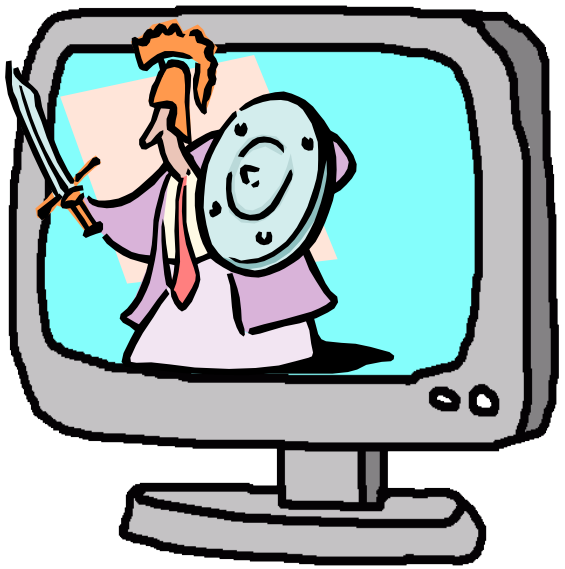
- 脆弱性（ぜいじゃくせい）の解消
- コンピュータウイルス対策
- 業務に関係のないアプリケーションはインストールしない（使わない）
- 私物パソコンは業務では使わない
- 業務情報のバックアップ

（1）脆弱性の解消

- Microsoft社Windowsの場合
  - Microsoft(Windows) Updateの実施（毎月定例）
- Apple社のMacの場合
  - 定期的なセキュリティ更新の適用
- パソコン上で利用するアプリケーション
  - 常に最新のバージョンあるいはセキュリティ更新を適用する

(2) コンピュータウイルス対策

- セキュリティ(ウイルス)対策ソフトを利用する
- ウイルス定義ファイル(パターンファイル)は常に最新にする(自動更新)
- 機能は安易に止めない
- ウイルスを発見したら駆除して報告

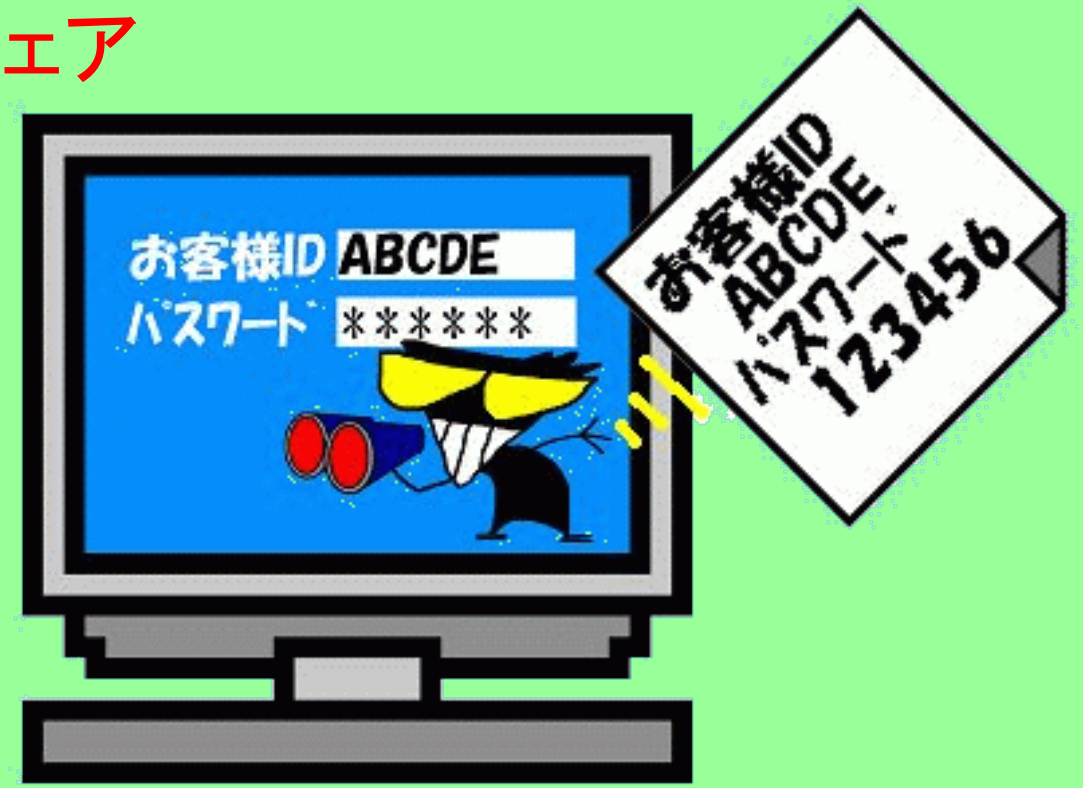


最近話題？のウイルス

- 情報を盗むスパイのようなウイルス
- 脅しをかけ、偽ソフトを売りつけるウイルス
- 人質？を取り、身代金を要求するウイルス
- 会議や私生活を盗撮するウイルス

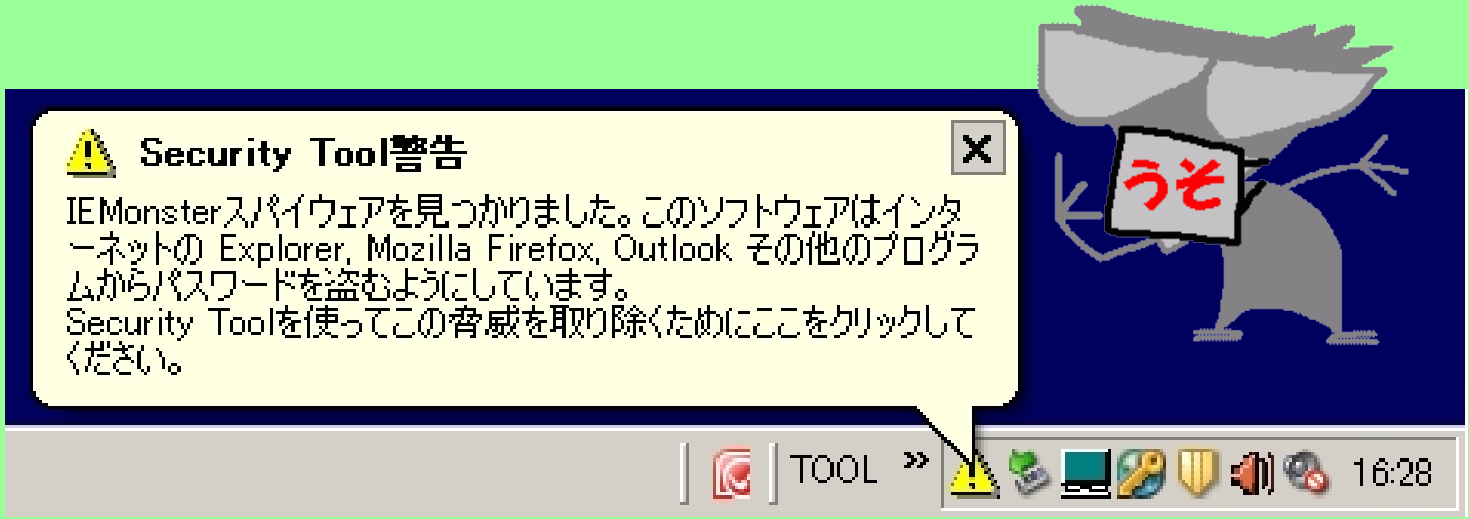
こんなウイルスも・・・

- キーボードの操作を記録･外部へ送信する
  スパイウェア



こんなウイルスも・・・

- 「ウイルスに感染してるよ!!」って自作自演のウイルス感染の嘘をつき、脅迫紛いに偽ウイルス対策ソフトを買わせるスケアウェア



こんなウイルスも・・・

- 「おまえのファイルを暗号化した!!パスワードが知りたければお金を払え!!」って、ファイルやフォルダを人質にとるランサムウェア
  - ランサム＝身代金

こんなウイルスも・・・

- 感染したPCのウェブカメラで盗撮するウイルス

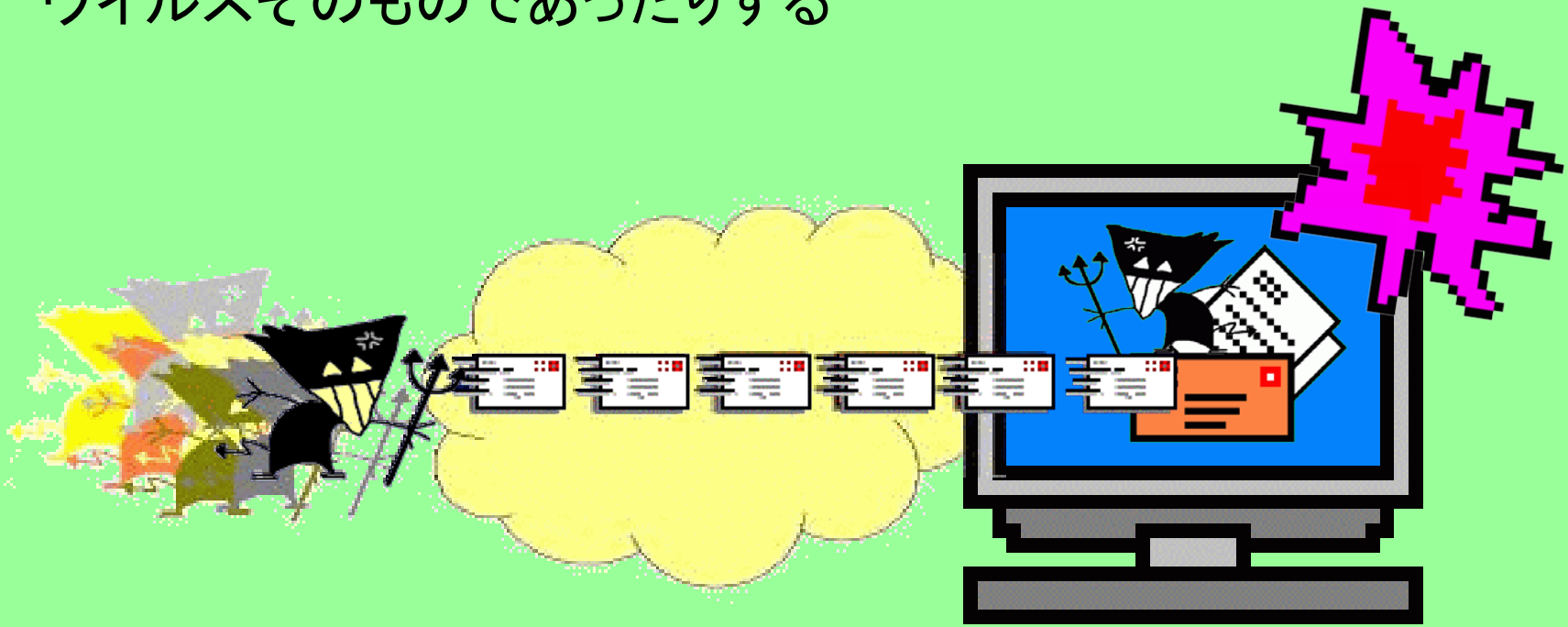
代表的なウイルスの感染経路

- メールからの感染
- ウェブサイトからの感染
- USBメモリからの感染

メールからの感染

- メールの添付ファイルを開くことにより感染

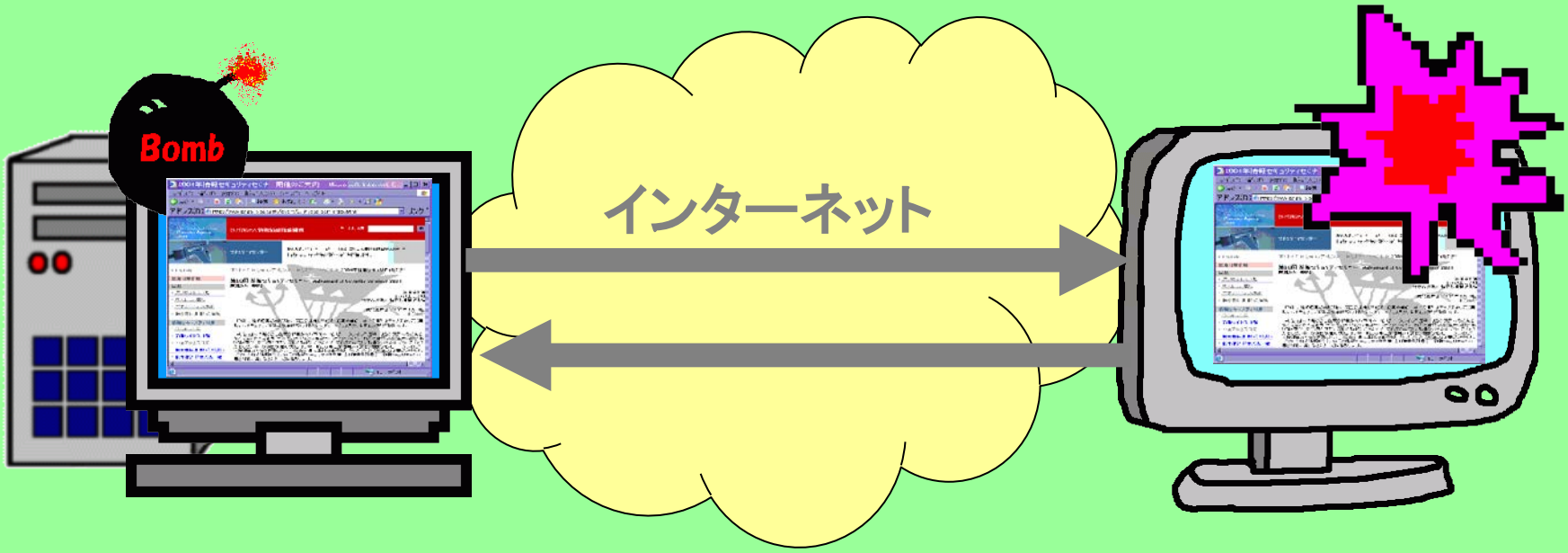
※添付ファイルがウイルスに感染していたり、添付ファイルがウイルスそのものであったりする



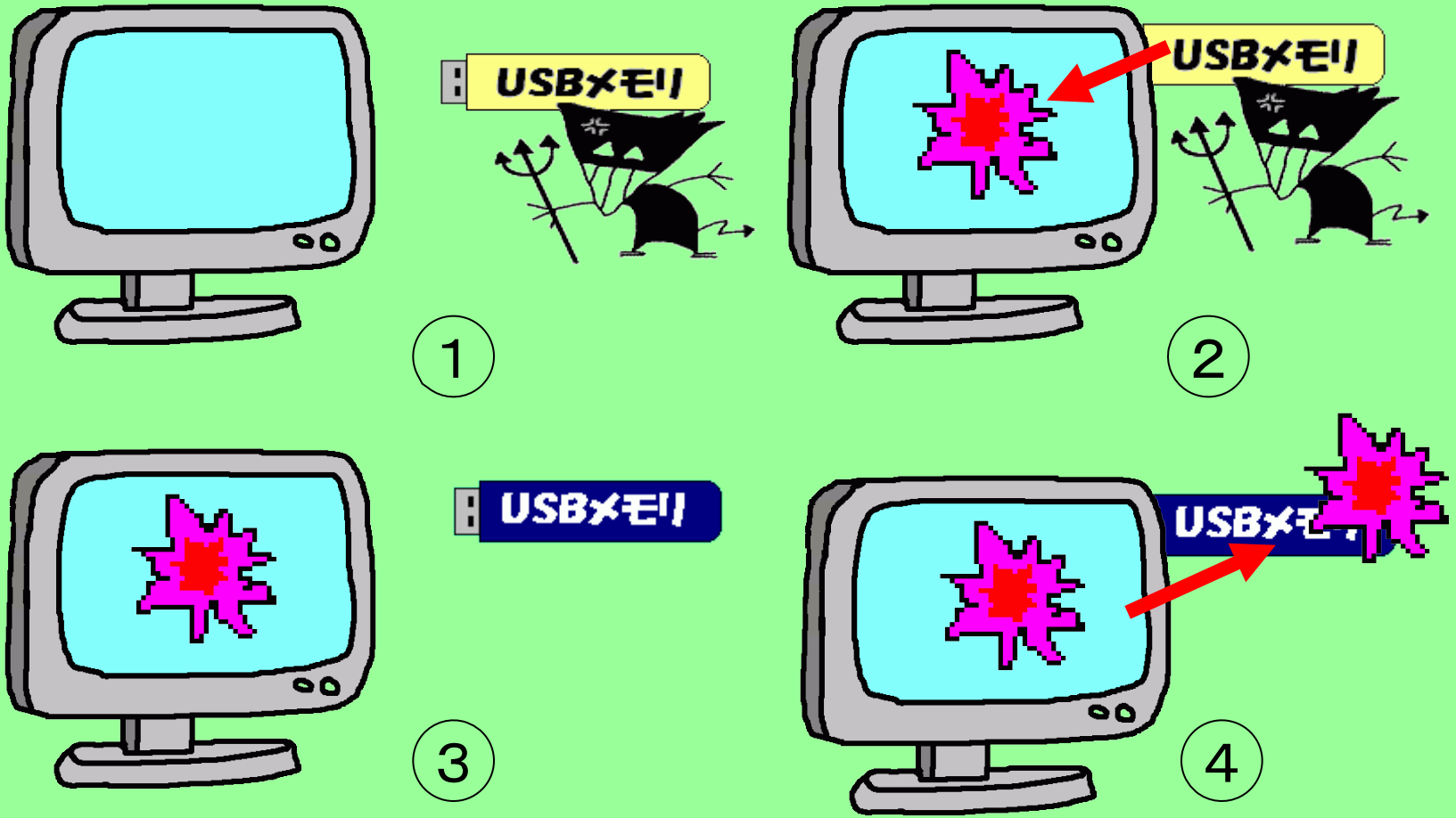
ウェブサイトからの感染

- ウイルスが仕掛けられたウェブサイトを閲覧することにより感染

  迷惑メール、IM（インスタントメッセンジャー）、SNS（ソーシャルネットワーキングサービス）やブログサイト、アダルトサイト等に記載された不正なリンクから悪意のあるウェブサイトに誘導され感染



USBメモリからの感染



細かいことを言えば…

自動実行（Autorun）による感染はMicrosoftの脆弱性対策で解消されつつあります（みんながパッチを適用していれば）が…

USB内に、利用者が興味を引くようにアイコンやファイル名を偽装された実行ファイルやウイルスに感染したファイルを置くことで、利用者自らに実行(開かせる)させる方法が増加しています（これはファイル交換でのウイルス感染に悪用された方法ですが最近話題の標的型攻撃メールにも使われています）

見た目はWordファイル（.doc）なのに、
実は実行（.exe）ファイルだったりします

（3）業務に関係のないアプリケーションは使わない

- ファイル交換ソフトに代表される、利用すると情報漏えいする可能性のあるアプリケーションは、企業内のパソコンでは使用してはいけません
- 自宅からゲームソフトを持ち込むのも、業務に関係ないのでNG
- 業務に関係ないサイトへの訪問も・・・

ファイル交換ソフトを介した情報漏えい

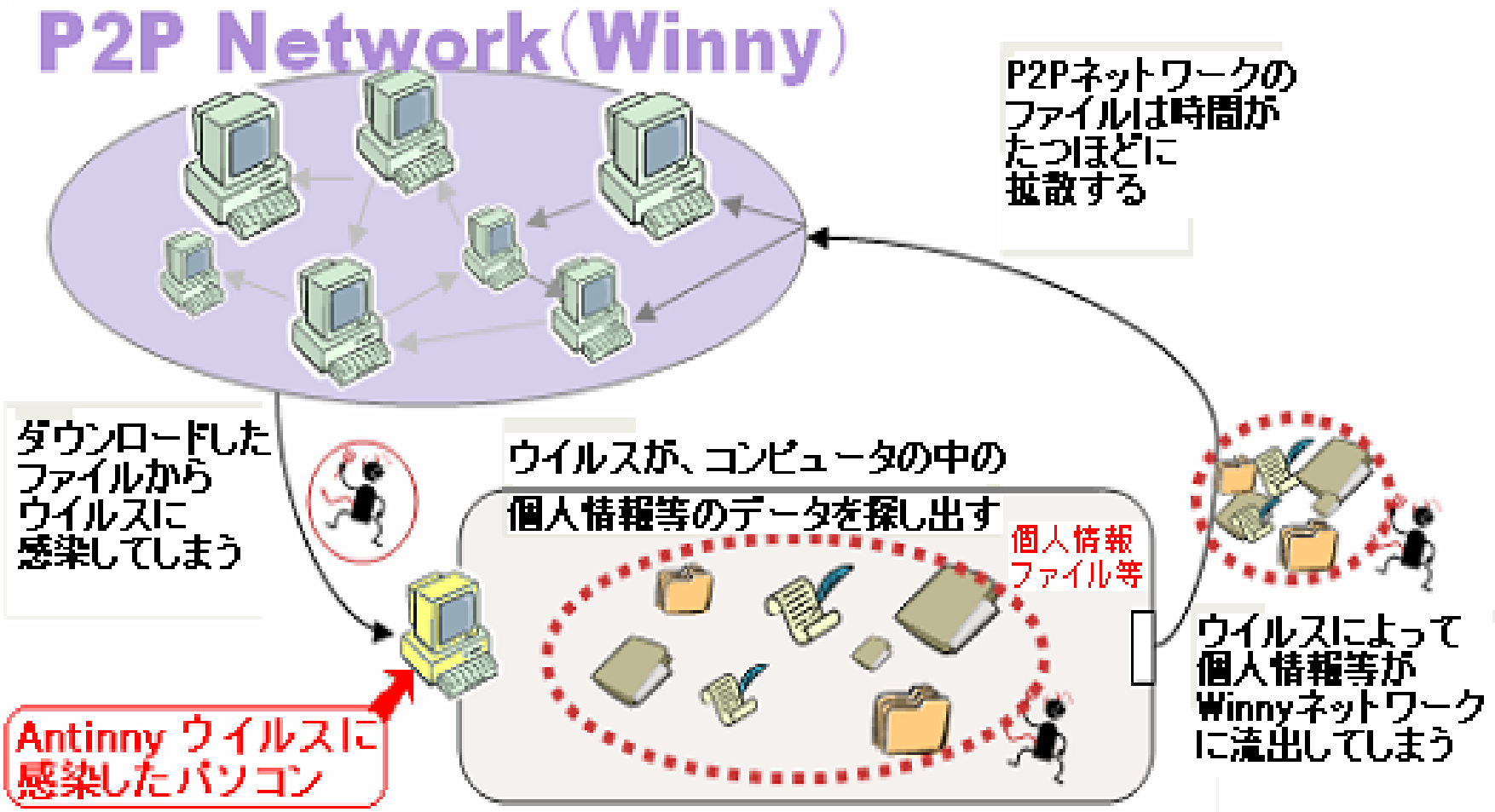


図 ファイル交換ソフトから情報流出する仕組み

仕事で使うと危ない・・・

- 情報漏えいを起こし易いファイル交換ソフト
- 仕事に無関係なソフト、誰も保障してくれないフリーソフト、私物ソフト
  - 脆弱性対策ができない（サポートされていない）
  - 情報を盗んだり、壊したりする不正なプログラムが入っているかもしれない（偽ウイルス対策ソフトなど）

（4）私物パソコンは業務では使わない

- 「業務に関係のないアプリケーションは使わない」と同じ理由で、私物パソコンは業務で使わないことが望ましい
- どうしても必要な場合は、上司の許可をとってから、十分なセキュリティ対策を施してから利用することになりますが、私物パソコンは企業として十分に管理できないので、原則として業務には使わないことを推奨します

最近の事情として言えば…

BYOD（Bring Your Own Device）

“自分の端末を持って来いよ” の話

自分勝手な BYOD はとても危険です

メリット(例えばコスト低減や効率の向上)もデメリット(例えば情報持ち出しによる情報漏えいの危険性の増加)もあります

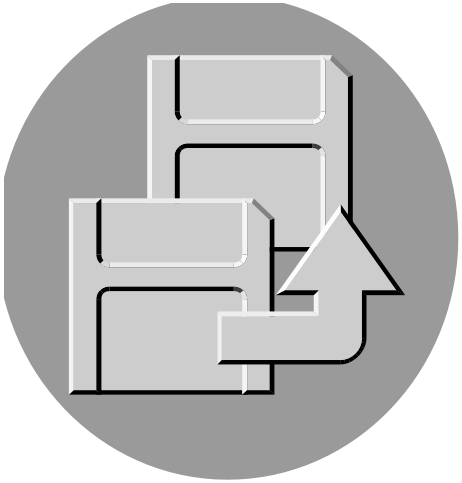
いろいろなところで試行錯誤中？

流れとしては、ITの将来像まで変えそうな勢いです…が…

今のところは、状況に合わせて
「会社として確認し、必要なら許可を・・・」
といった話で考えられているようです

(5) 業務情報のバックアップ

- 故障や誤操作などにより、パソコンの中に保存したデータが、消えてしまうことがあります
- 定期的にバックアップを取得しておけば、このような不測の事態に備えることができます



対策7：パスワード・・・

- パソコンやスマートフォン、携帯電話を利用する際のログインパスワードや暗証番号だけでなく、インターネットを利用していると多くのパスワードが必要になってきています
- 安易なパスワードやパスワードの使いまわしなど、パスワードの運用･管理上危険な取り扱いを多く見受けます

パスワードの掟(おきて)

- 他人に推測されやすいパスワード（ニックネームや誕生日等）は使わない
- 大文字・小文字・数字・記号の組み合わせ
- 長いパスワード(推奨は８桁以上)
- 推測しづらく自分が忘れないパスワード
- 他人の目に触れるような場所に、パスワードを残さない
- 定期的に変更する

パスワードの掟2

- パソコンのログインパスワードは、他人に推測されないようなある程度の強度を持つパスワードを設定しよう
- パソコンのログインパスワードは、他人に知られた場合は速やかに変更しよう
- インターネット上のサービスを利用するためのパスワードは、ある程度の強度を持たせ、定期的に変更しよう
- インターネット上のサービスを利用するためのパスワードは、サービス提供側で漏えい事故が発生した場合は、速やかに変更しよう
- インターネット上のサービス毎に異なったパスワードを設定しよう
- **忘れそうなら、紙に書いて大事に保管**

対策7：電子メール・・・

- 業務における電子メールの利用は、やり取りする内容自体が重要な情報なので、**宛先を間違えるなどの誤送信は、絶対にあってはなりません**
- 誤送信を防ぐためには、以下のような対策が必要
  - ☑送信前に宛先と内容の再確認
  - ☑重要な情報はメール本文ではなく暗号化された添付ファイルに…
  - ☑同時に多くの宛先に送信（同報メール）する場合は、ToやCCでいいのかBCCにすべきなのか良く考えるましょう

対策8：守秘義務って何・・・

- 企業にとって重要な情報は、従業者であれば、対外的に秘密としなければなりません
- それが**守秘義務**です
- 一般的には、採用の際に守秘義務があることを知らせるなどのように、企業は従業者に機密を守らせているはずです

「3つのかばん」のお話…

啓発ビデオ放映

まとめ

- 「自分の身は自分で守る」
- 「会社の身も自分が守る」

ただし、自分ひとりで解決×
→報・連・相が大事

参考情報の紹介

IPA対策のしおり

http://www.ipa.go.jp/security/antivirus/shiori.html

情報セキュリティ対策の基礎知識（DVD-ROM）

情報セキュリティ対策の啓発ビデオ

- 情報セキュリティ　普及啓発　映像コンテンツ

  http://www.ipa.go.jp/security/keihatsu/videos/

- YouTube：IPAチャンネル

http://www.youtube.com/ipajp/

ここからセキュリティ！

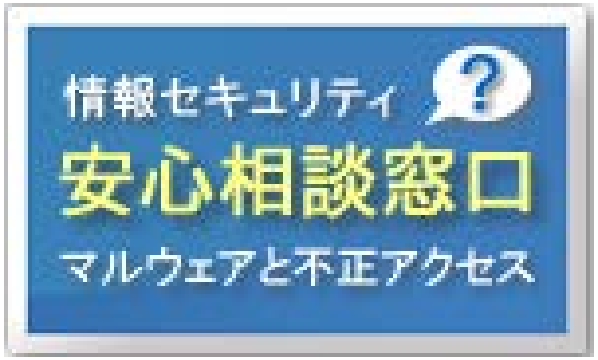
http://www.ipa.go.jp/security/kokokara/

I ♥ スマホ生活

IPA

http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/

情報セキュリティ安心相談窓口



電　話　**03-5978-7509**
(オペレータ対応は、平日の10:00～12:00 および 13:30～17:00)

E-mail　**anshin@ipa.go.jp**
※このメールアドレスに特定電子メールを送信しないでください。

FAX　**03-5978-7518**

郵　送　〒113-6591
東京都文京区本駒込2-28-8
文京グリーンコート　センターオフィス16階
IPAセキュリティセンター　安心相談窓口

5分でわかるITパスポート

https://www3.jitec.ipa.go.jp/JitesCbt/index.html

ご清聴ありがとうございました

独立行政法人 情報処理推進機構
技術本部セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込2－28－8
　文京グリーンコート センターオフィス16階
TEL 03（5978）7508　FAX 03（5978）7518
電子メール　isec-info@ipa.go.jp
URL　http://www.ipa.go.jp/security/