IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2007. 2. 14
重要インフラセキュリティセミナー

セキュリティインシデントを考慮した事業継続管理（BCM）

IT : Information Technology
BCP : Business Continuity Plan
BCM : Business Continuity Management

独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan (IPA)
セキュリティセンター　情報セキュリティ技術ラボラトリー長

（(株) 日立製作所 情報・通信グループ　セキュリティ事業部
セキュリティソリューション推進本部　統括主査
Hitachi Incident Response Team 主幹アドバイザ）

小林　偉昭
hd-koba@ipa.go.jp

HIRT Hitachi Incident Response Team

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

本日の話のストーリー

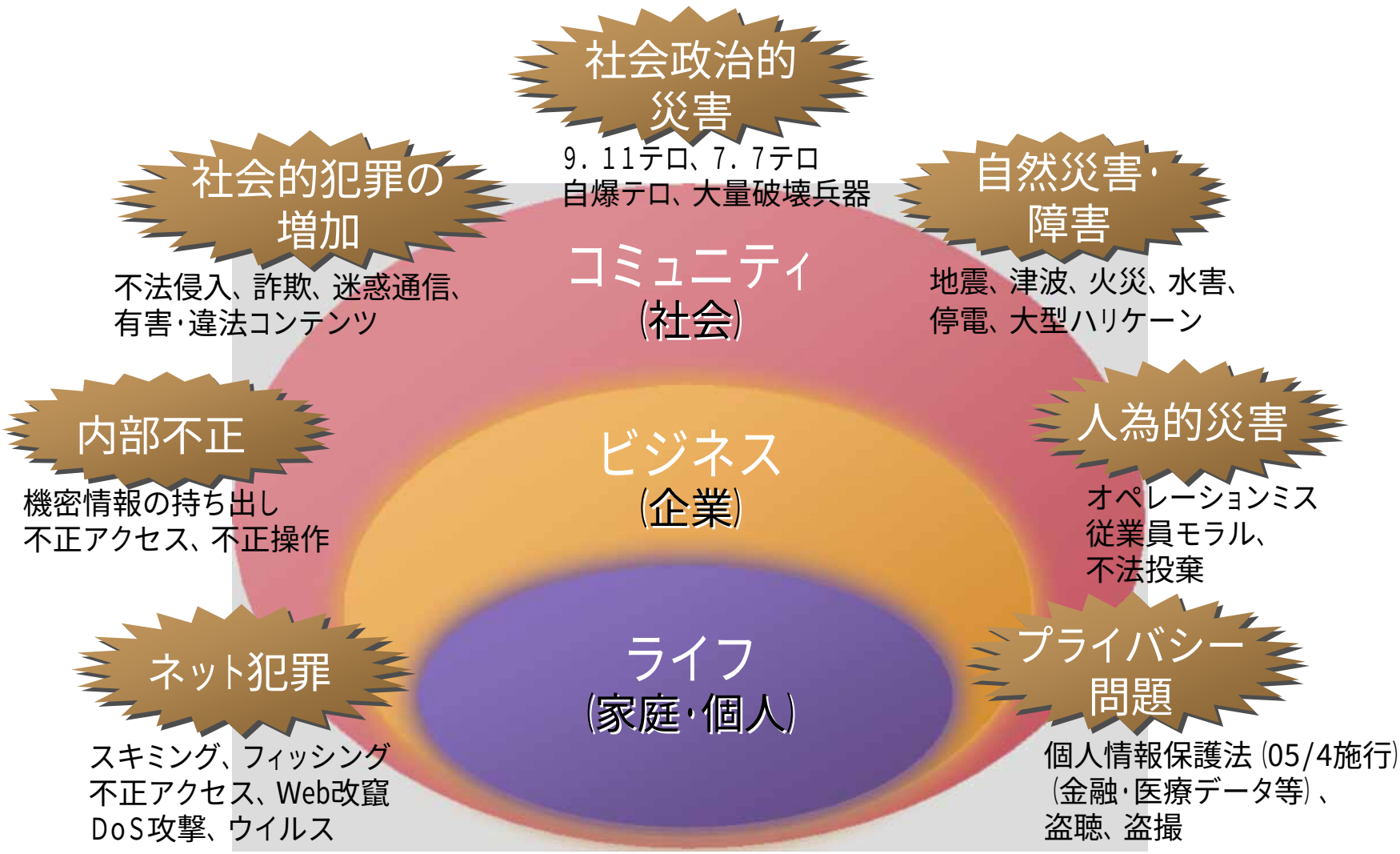
1．はじめに
　IT依存の進展
　BCP/BCMとは
2．セキュリティインシデントとBCM
　IT脆弱性とは
　ITの脆弱性取り扱いの状況
　具体的な脆弱性事例
　ITの脆弱性へのBCM適用例
　BCMベストプラクティスまとめ
3．まとめのようなもの

1．はじめに
IT依存の進展
BCP/BCMとは

BCP : Business Continuity Plan
BCM : Business Continuity Management

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

多様化するリスク



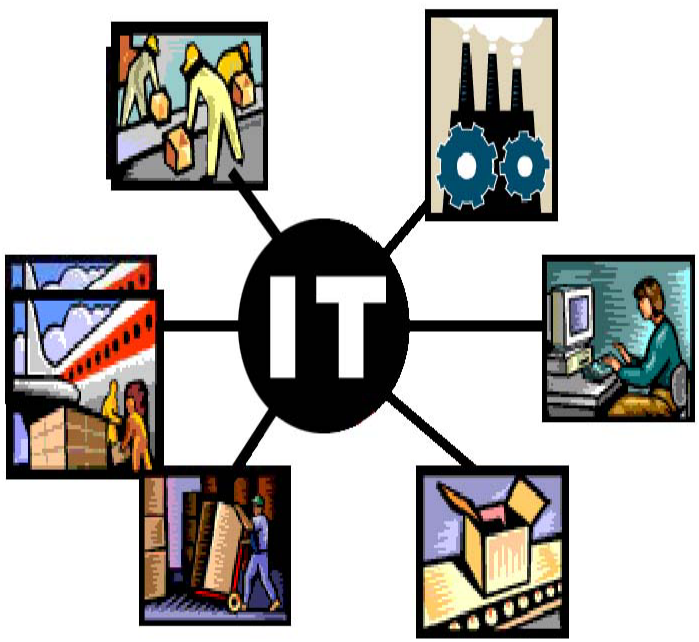
「不安解消」、「安心･安全の確保」に対する社会的ニーズ増大

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報システムITのパラダイムシフト

「システムを止めない」→「ビジネスを止めない」

電力、水道、運輸、金融、情報通信等の重要インフラを利活用している日常生活や経済活動を持続する上で、今や情報システムITの安定的な継続稼動は欠かせない。



障害や災害等の発生による情報システムITの大規模な停止を回避し、データを守り、速やかに回復させるだけでなく、ビジネスの重要なプロセスについては可能な限り停止しない、できれば一瞬たりとも停止しないことが、ビジネス継続の観点から注目されている。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, J

BCPとBCMの定義

Business Continuity Plan & Business Continuity Management

BCP：潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする事業計画。事故発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物。

BCM：組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランド及び価値創造活動を守るため、復旧力及び対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス。

参考文献等

事業継続策定ガイドライン（経済産業省）（2005年3月）
http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf

事業継続ガイドライン第一版（内閣府中央防災会議）（2005年8月）
http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf

中小企業BCP策定運用指針（中小企業庁）（2006年2月）
http://www.chusho.meti.go.jp/bcp/

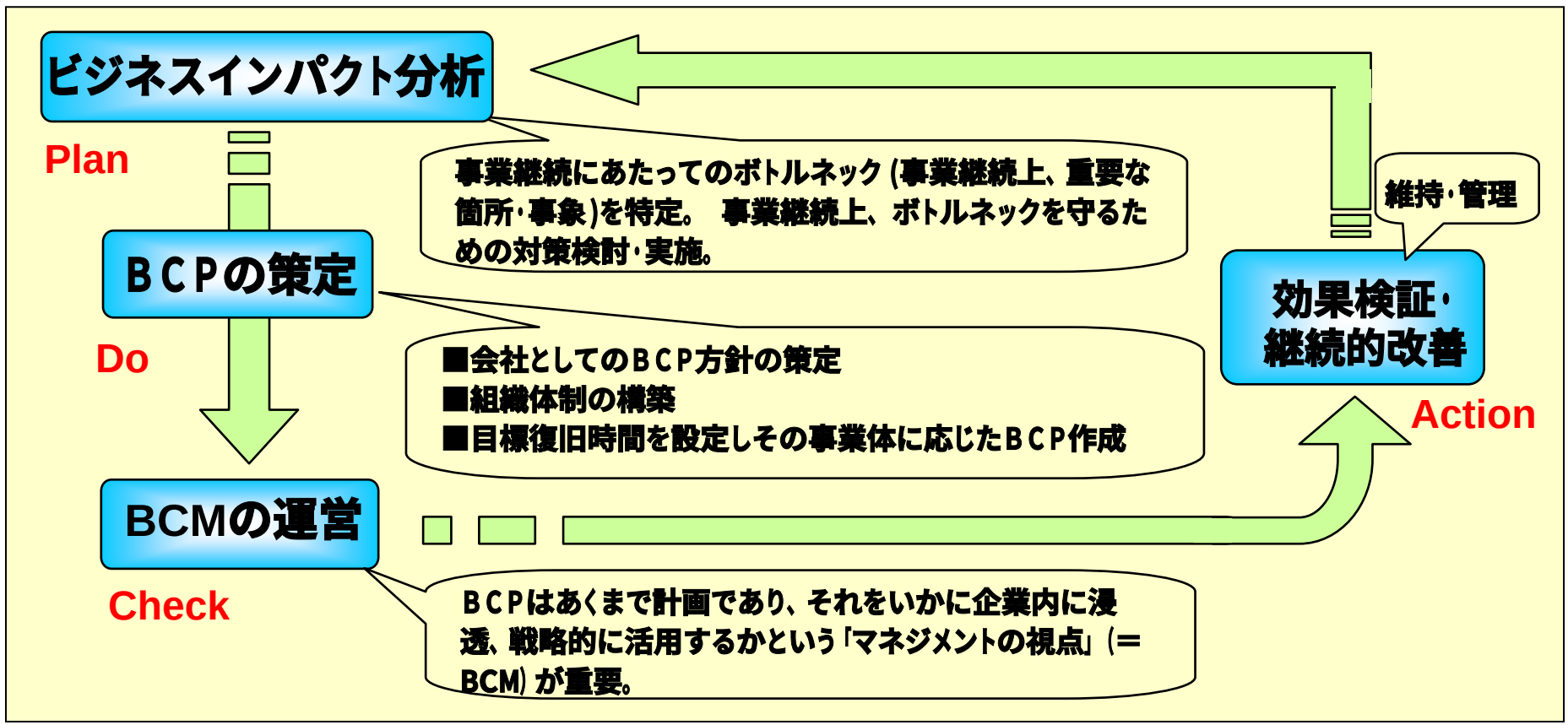
ビジネス継続性技術調査報告書(情報処理相互運用技術協会）（2005年3月）
http://www.net.intap.or.jp/INTAP/information/report/16-business-report.pdf

特定非営利活動法人　事業継続推進機構
Business Continuity Advancement Organization
http://www.bcao.org/

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCPの構築・運用のPDCAサイクル

PDCAサイクル：「計画（Plan）」「実施（Do）」「監視（Check）」「改善（Action）」のマネジメントサイクルとして捉え、組織運営を通じて継続的な改善を図る取り組み

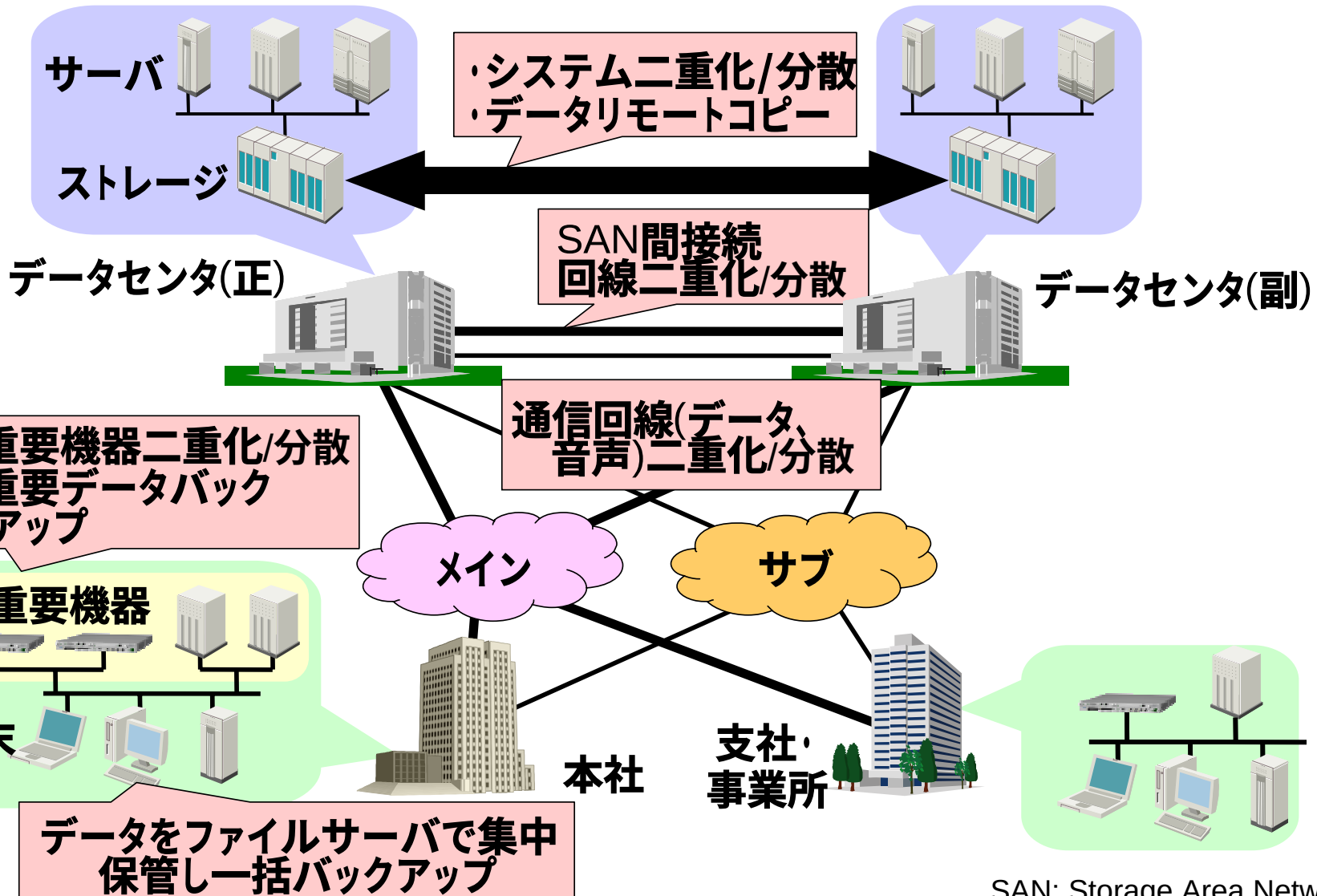


出典：経済産業省報告書

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ITシステムの災害・障害対策ポイント

ITシステム構成イメージ



SAN: Storage Area Network

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ビジネスプロセスの脆弱性分析（BIA：ビジネスインパクト分析）

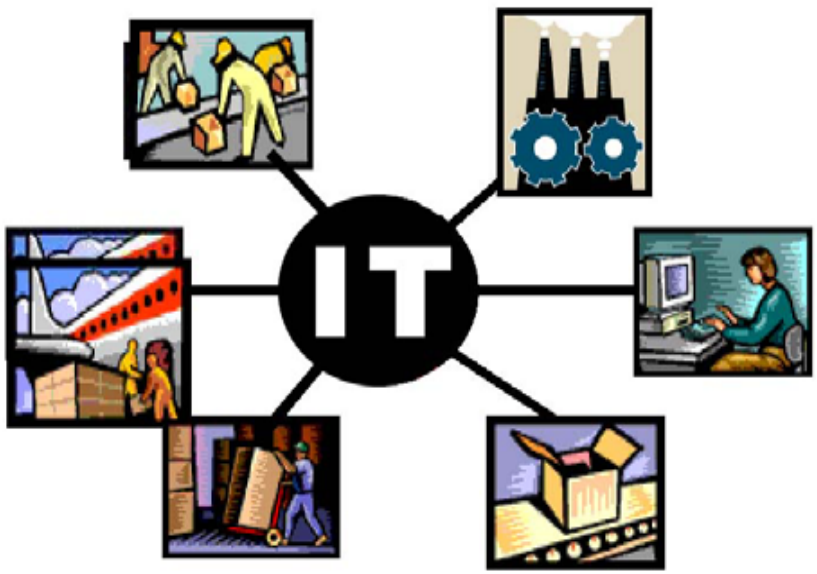
ITへのビジネスプロセス依存進展

→

ITの脆弱性分析

インターネットの普及・発展

人口普及率：66.8%（8,529万人。2005.12末現在）
ブロードバンド加入者：2,330万加入（2006.3末現在）

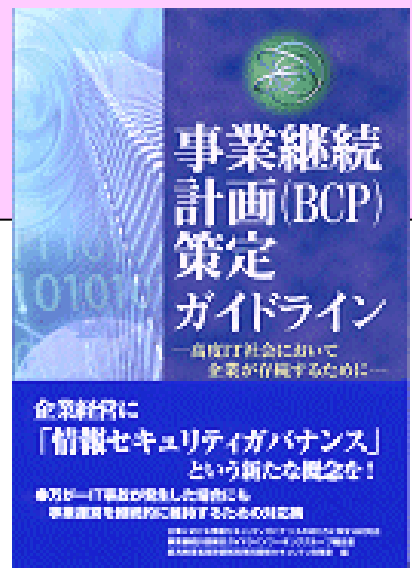


社会経済活動のIT化の進展

2004年電子商取引の市場規模拡大
企業間：102.7兆円（前年比33%増）、消費者向け：5.6兆円（前年比28%増）

個別事象への脆弱性分析適用

大規模なシステム障害
セキュリティインシデント
情報漏えい・データ改ざん
その他



IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

セキュリティインシデントへの対応

BCP/BCM適用範囲とビジネスインパクト分析（例）

適用範囲：

・**ソフトウエアの脆弱性を悪用**した不正アクセス、コンピュータウイルス感染やWeb改ざん等により業務の停止・低下、個人情報の漏洩や情報の改ざんなどの発生により顧客・協力会社や社会から信頼を失い、経営に重大な影響を及ぼすことを想定したBCPを策定する。

ビジネスインパクト分析：

・本BCPで対象とする情報システムは、たとえば、オンラインショッピングサイト等を決める。

個々の情報システムの目標復旧時間（RTO）の設定。たとえば、システム停止をしてから脆弱性対策を実施し、システム再開までの目標復旧時間を決める。4時間とか1日。

2．セキュリティインシデントとBCM

脆弱性とは
ITの脆弱性取り扱い状況
具体的な脆弱性事例
ITの脆弱性へのBCM適用例
BCMベストプラクティスまとめ

BCM : Business Continuity Management

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティに関する新たな脅威に対する意識調査

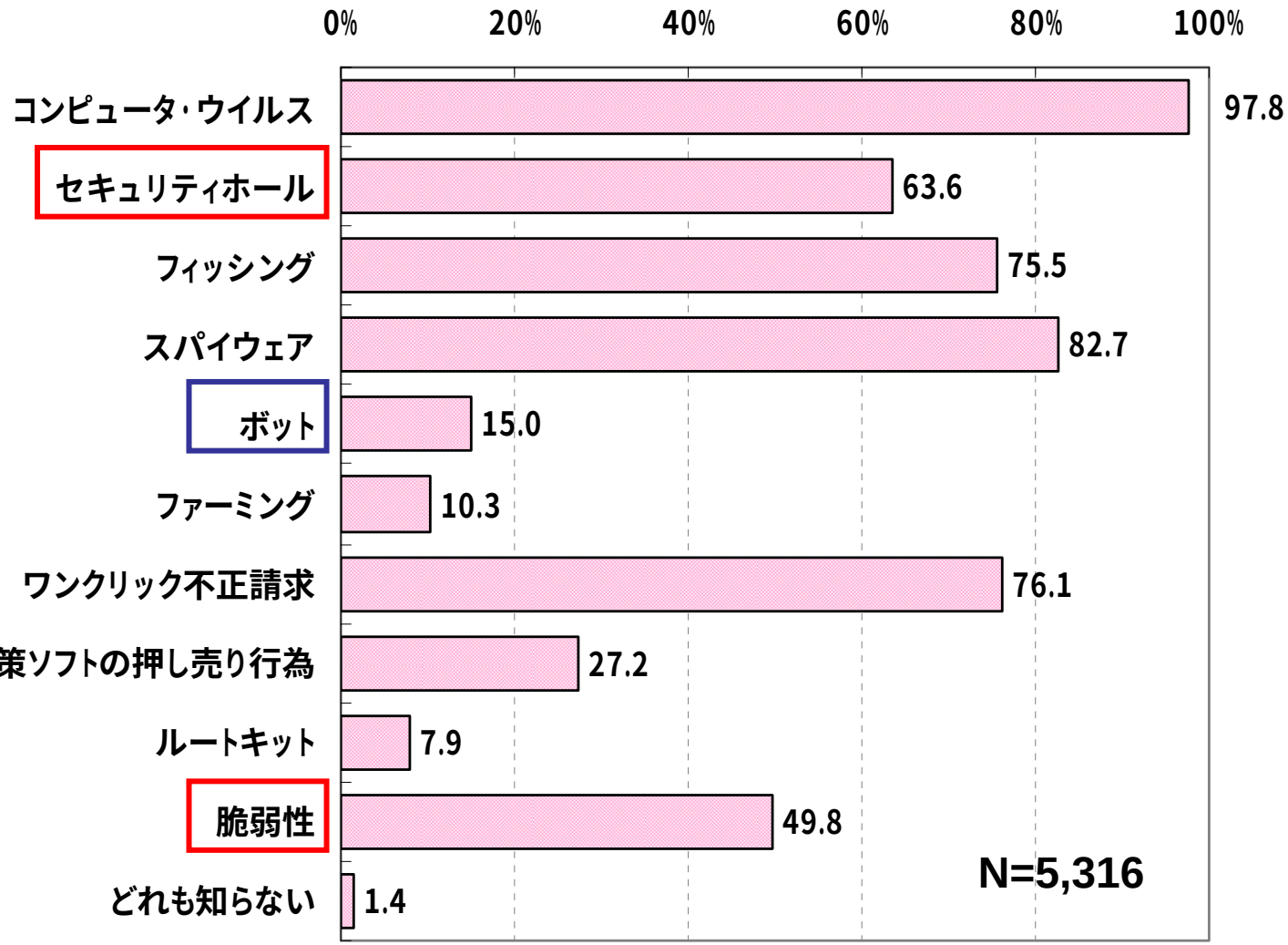
情報セキュリティに関する言葉の認知度　[回答者全体]（複数回答）

調査方法 ： ウェブアンケート調査　　調査期間 ： 2006年11月15日～11月16日
調査対象 ： 15歳以上のPCインターネット利用者

情報セキュリティに関する言葉の認知度

聞いたことがあるものをすべて選んで回答。最も認知度が高いのは「ウイルス」97.8%、次いで「スパイウェア」が82.7%。「ボット」は15.0%で低い。

「セキュリティホール、脆弱性」聞いたことがあるのはインターネットユーザのほぼ半分



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

脆弱性の定義

脆弱性（ぜいじゃくせい）とは

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。
ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

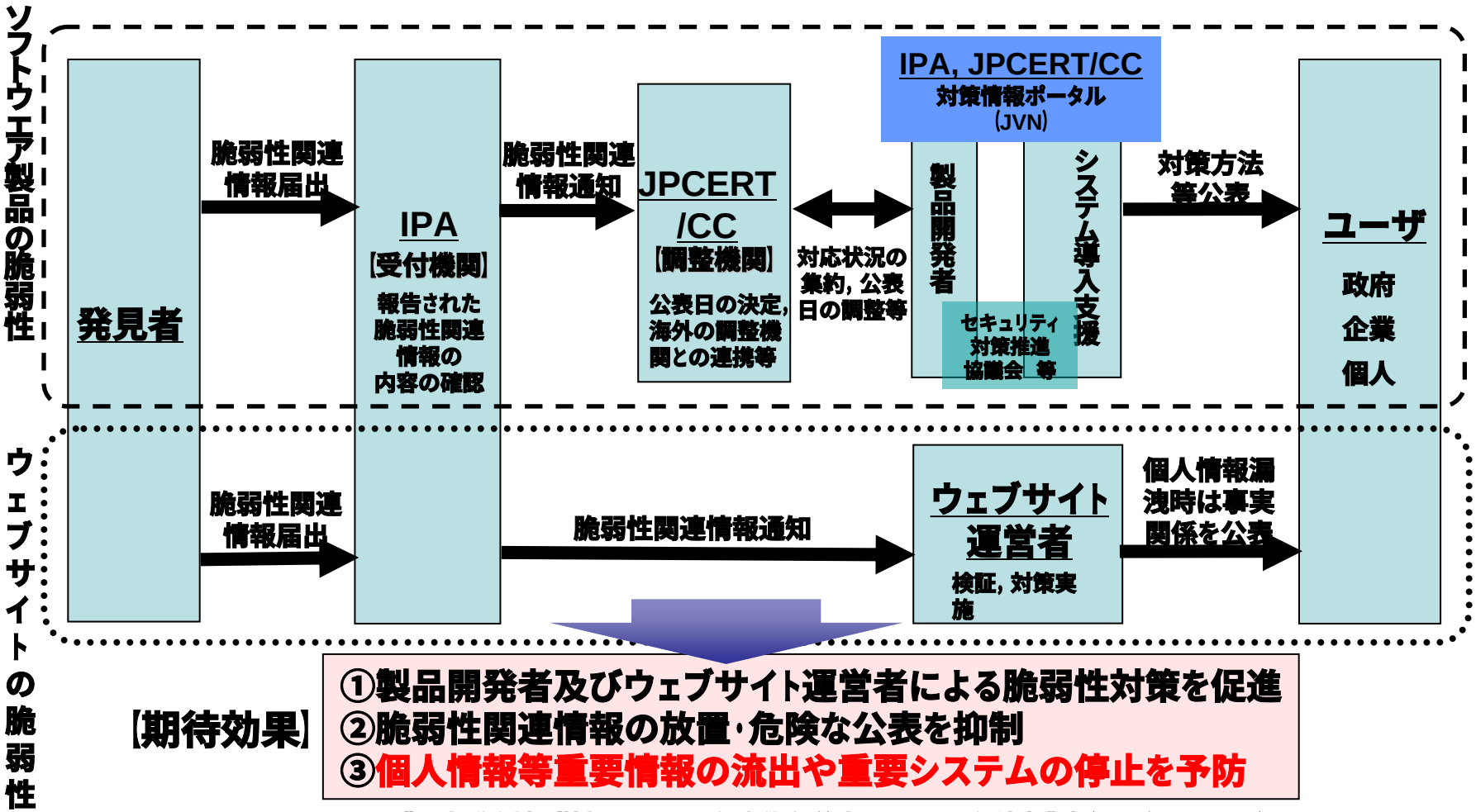
「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示 第235号）

セキュリティホールとも呼ばれる。近年、脆弱性がコンピュータウイルスや不正アクセス等の攻撃に悪用されるケースが増加。脆弱性に関する情報の公開後に、その脆弱性を狙う攻撃手法が作られ、流布するまでの期間が短くなる傾向。さらに、脆弱性情報の公開前に攻撃が行われる脅威（「ゼロディアタック」）も増している。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティ早期警戒パートナーシップ

個人情報等重要情報の流出や重要システムの停止を予防



【期待効果】

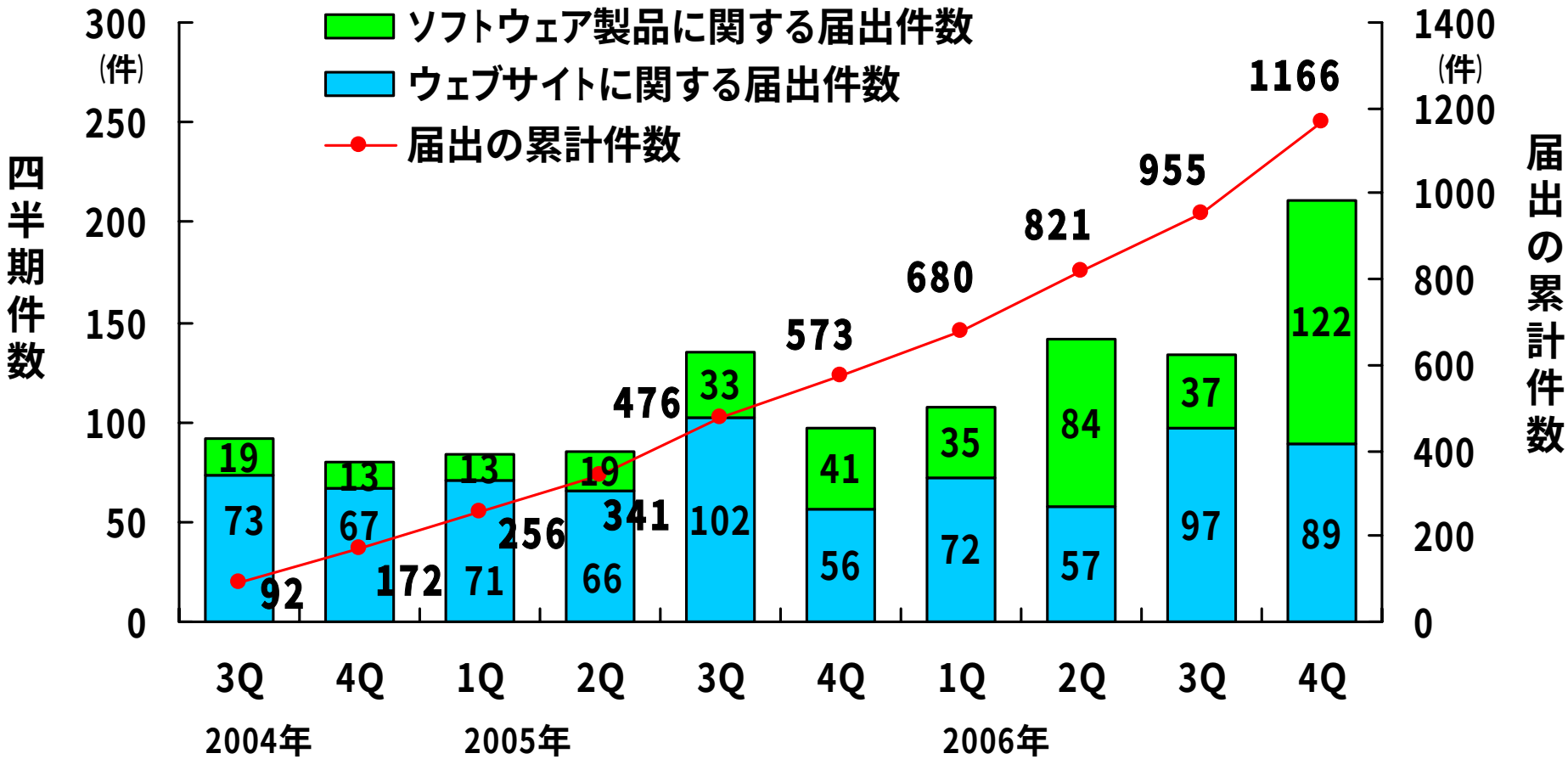
①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②脆弱性関連情報の放置・危険な公表を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

出典： 報道資料”「情報セキュリティ総合戦略」策定について”，経済産業省 (2003年10月10日)

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

脆弱性の現状：脆弱性関連情報の届出件数の推移

脆弱性の届出件数の四半期別推移
2006年10月24日に1000件に達した。



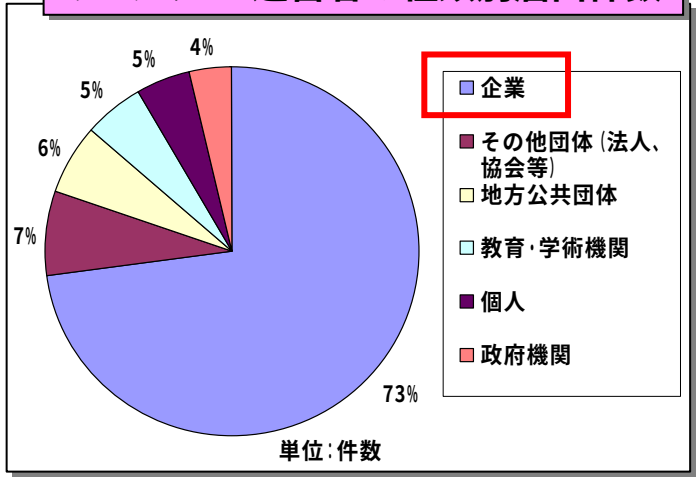
2004年7月から受付開始

ウェブサイトの脆弱性種類別内訳

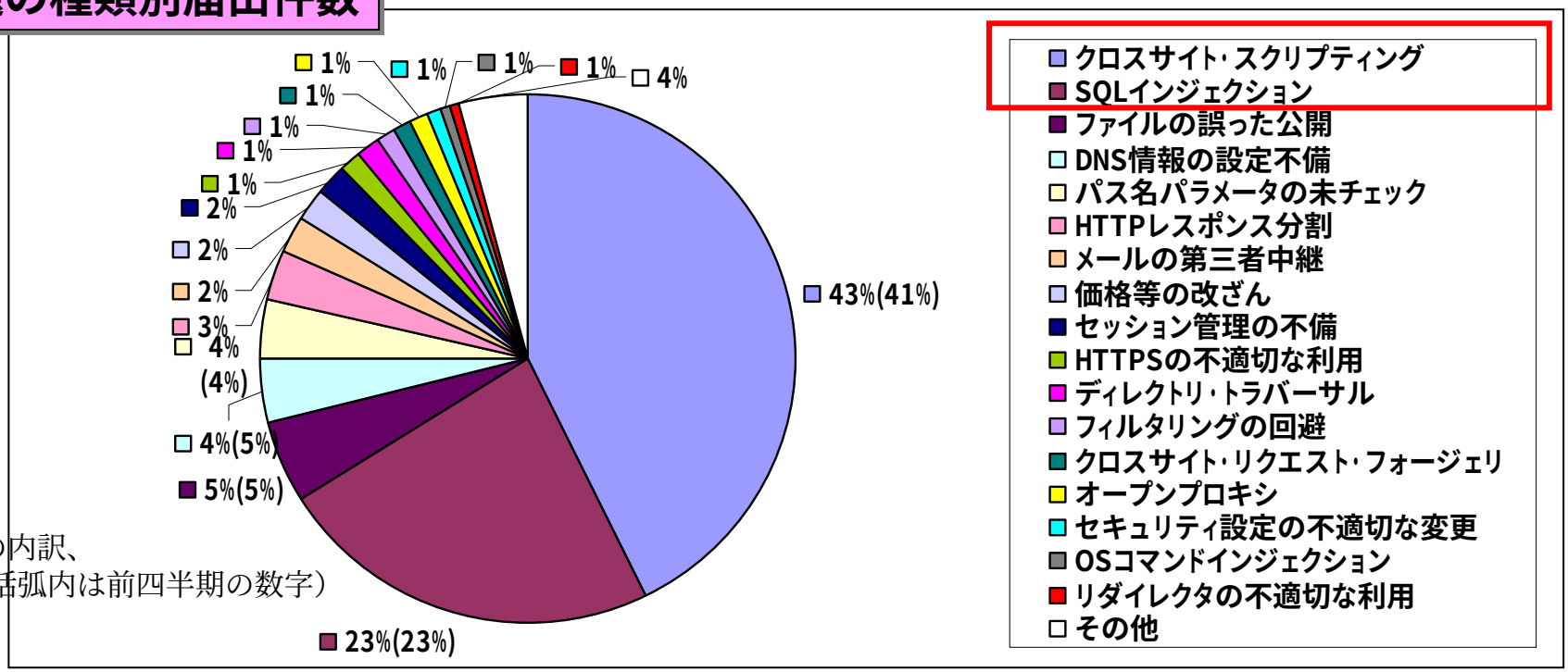
(届出受付開始から2006年12月末まで)

- クロスサイト・スクリプティングの問題に関する届出が最多(43%)。SQLインジェクションの問題も多い(23%)。
- 届出全体の約3/4は、企業ウェブサイトの問題。

ウェブサイト運営者の種類別届出件数



問題の種類別届出件数

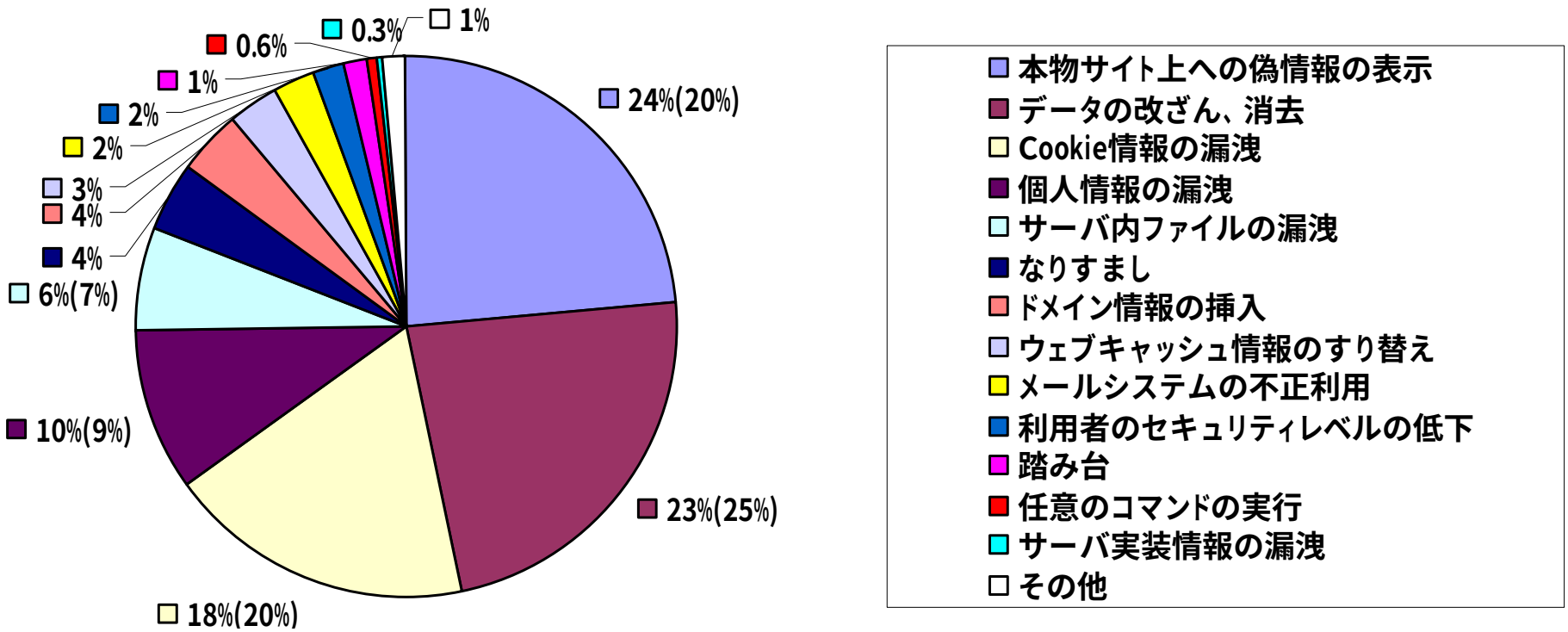


(704件の内訳、
グラフの括弧内は前四半期の数字)

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ウェブサイトの脆弱性脅威別内訳

（届出受付開始から2006年12月末まで）



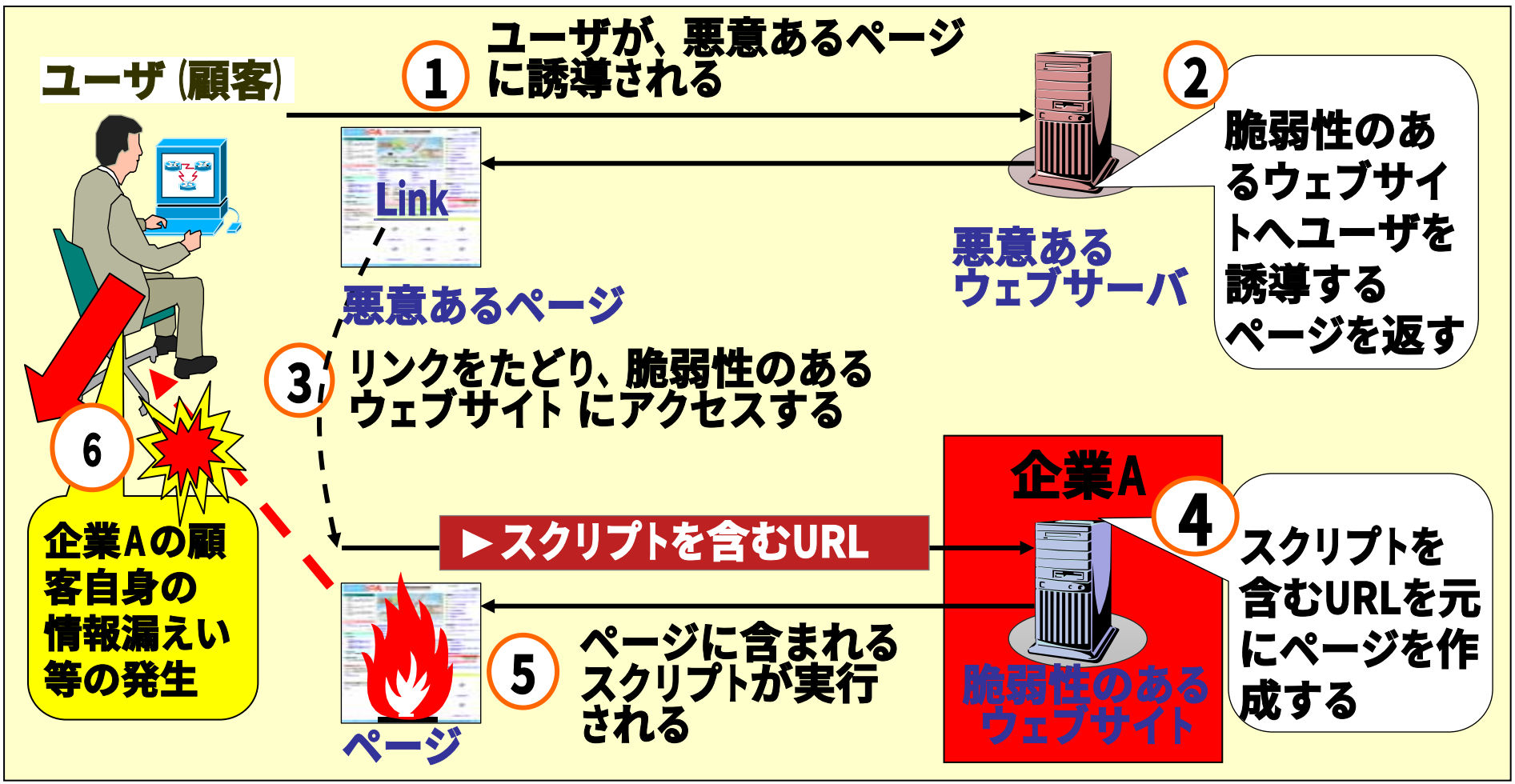
「クロスサイト・スクリプティング」の脆弱性の脅威としては、「本物サイト上への偽情報の表示」、「SQLインジェクション」の脆弱性の脅威としては「データの改ざん、消去」が多い。

ウェブサイト運営者は、「信頼される企業」として脆弱性を作り込まない、作り込ませない対応が必要。

事例1：クロスサイトスクリプティング（その1）

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

原因：ウェブページを出力する際の処理が不適切
脅威：攻撃者により認証情報の盗難や詐欺ページを表示するスクリプトを埋めこまれる
影響：問題のあるウェブサイトに接続しているユーザの認証情報の盗難、ユーザのブラウザ上に偽ページを表示する（フィッシング詐欺）



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

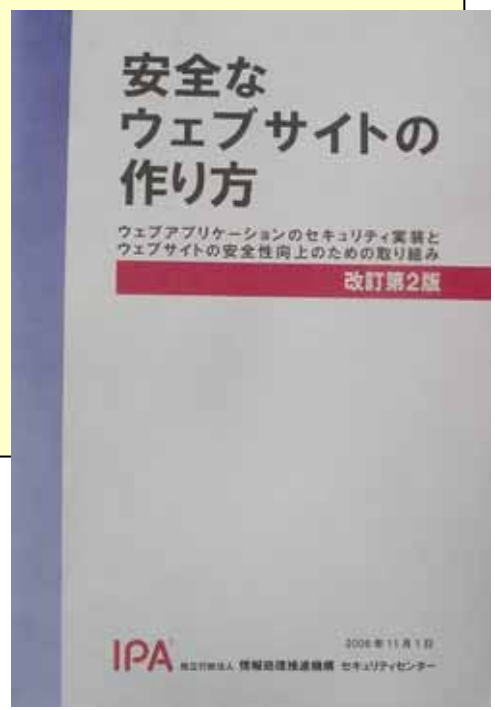
事例1：クロスサイトスクリプティング（その2）

顧客へ損害：ブランドへのダメージ(信頼できない企業)

被害：Webサイト自身ではなく、企業AのWebサイトのページ閲覧者に発生
→顧客やステークホルダー及びポテンシャル顧客へ被害を与える可能性
→閲覧者ブラウザ（パソコン）から個人情報や機密情報他を漏えいする可能性

対策1：企業AのWebサービス停止が、被害拡大防止には望ましい。
➔ユーザ掲示板のようなサービスであると事業への影響は少ないが、
オンラインショッピングサイトを停止することは事業全体に影響を及ぼす。

対策2：Webアプリケーションの脆弱性対策の実施。
➔脆弱性の指摘対応時の対策：
予算確保や発注先との契約への考慮が必要。
たとえば、IPAの「安全なWebサイトの作り方」
で指摘された事項に全て対応することを
発注仕様書に入れるのが望ましい。
また、セキュリティベンダによる監査も望まれる。

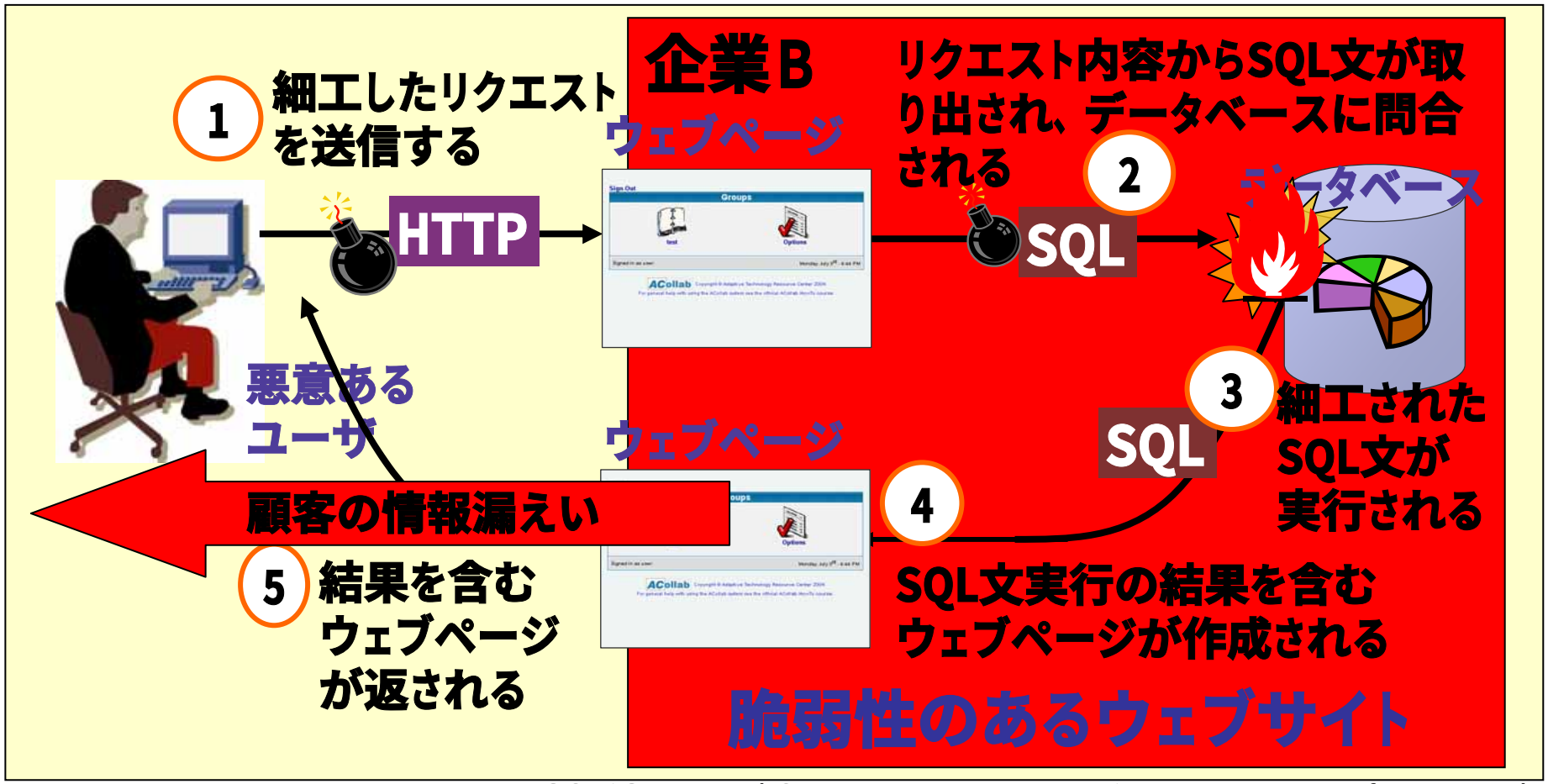


「安全なウェブサイトの作り方　改訂第2版」2006.11.1
http://www.ipa.go.jp/security/vuln/websecurity.html

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

事例2：SQLインジェクション（その1）

原因：ユーザからのリクエストの処理方法が不適切
脅威：攻撃者によってデータベースを操作される
影響：データベースの秘密情報の漏洩、データベースに登録されている情報の破壊、内部ネットワークに接続されているサーバを攻撃するための踏み台



SQL：Structured Query Language　HTTP：Hyper Text Transfer Protocol

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

事例2：SQLインジェクション（その2）

2005年企業における情報セキュリティ事象被害額調査結果について
調査の結果　（不正アクセス(SQLインジェクション)）

推計される被害額（事例からの推計）：

復旧対策　**システム再構築関連**　4,800万円～1億円
（Webアプリの改修、第三者によるセキュリティ検査等）
事象対応社内人件費 180万円～360万円
(組織のトップを含めた専門対応チームの設置等)

対外経費　**問合わせ窓口等**　数百万円～5千万円
(顧客への謝罪、問合わせ窓口設置、保証等)

以上、対策経費自体で**総額1億円を越えるケース複数あり**

売上減　数ヶ月間閉鎖により、**数億円から数十億円の減**

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

事例2：SQLインジェクション（その3）

2005年企業における情報セキュリティ事象被害額調査結果について
不正アクセス(SQLインジェクション）被害対応の実態

①事象の顕在化

自ら、ウエブサイト管理外注先等が改ざんを発見、アクセスログに異常なアクセスがあることを発見。直ちに、被害拡大防止のためサイトの全面的停止

②被害状況の調査

専門業者などにより被害原因調査。その結果、SQLインジェクションの脆弱性存在の発見。被害範囲の特定(個人情報の漏えいの有無など）。平均数日間。

③復旧作業

ウエブアプリ、データベース操作・管理ソフトの全数チェック、改修、サーバ再構築の実施。サイト再開に向けてセキュリティ専門企業による診断実施。数ヶ月間。

④対外説明等

顧客への事情説明、コールセンター設置、有償で広報等をしている企業においてはクライアントへの補償など。（リスクコミュニケーション）

⑤社内体制の整備

全ての復旧作業、対外説明が終了後、社内のセキュリティ対策部署の新設強化。

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

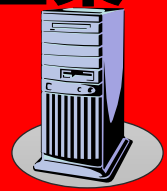
事例3：BOTの脅威（その1）

企業Xの利用ユーザ

自分の責任：
ウイルスメールの添付ファイル、
スパムメールのリンク先画像クリック
自分のPC内の脆弱性への攻撃

企業Xの
ウエブ利用

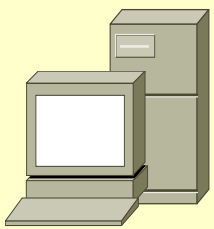
企業X　脆弱性のある
ウェブサイト



ボット
感染

悪意を持つ人からの指令により
対象サイトへ一斉攻撃が始まる

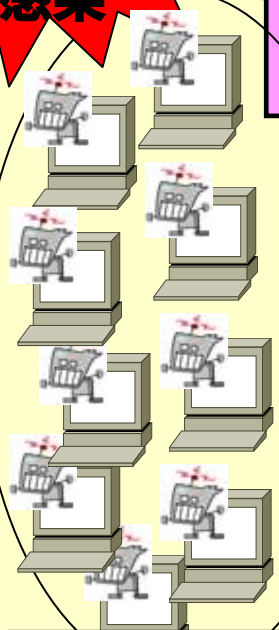
指令サーバ



各種指令

・感染活動
・サービス拒否攻撃
・迷惑メール配信
・スパイウェア
・自己機能の更新
など

悪意を持つ人

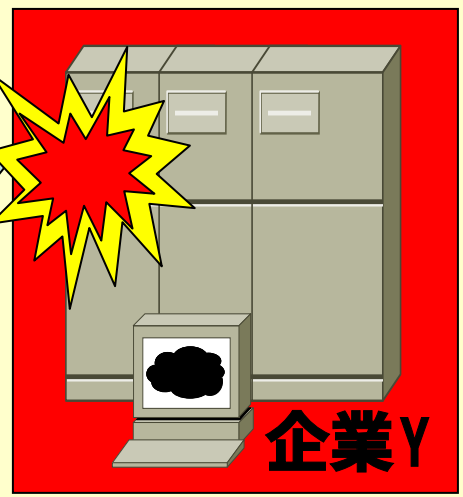


ボットネット

インターネット利用者

一斉攻撃

被害を受ける企業



企業Y

攻撃対象サイト

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

事例3：BOTの脅威（その2）

ボットによる感染被害状況

●「ボットネット」による被害としての推計は存在しないが、

①・**スパムメール**による2005年の被害額は、全世界で500億ドル、うち日本が50億ドルと推計（米Ferris Research社）。
・米国最大手のISP(AOL)によれば、スパムメールの75%（推定15億通/日）がボットから送信されている（2005年）。
・また、スパムメールの半数以上はボットネットによるものと推計（Sophos社）。

②**フィッシング**による2004年後半から2005年前半の被害額は、米国で27億ドルと推計（米Gartner社）。

③**DoS攻撃**による被害累計額は、米国で10億ドル超と推計（米Forrester Consulting社）。

④shadowcrewと呼ばれる**ボット運営組織**は、米・英・露・西・伯に4000人のメンバーを擁し、クレジット詐欺等により数百万ドルを稼ぐ。

⑤米マイクロソフトによれば、米連邦政府の2000台以上のPCがrootkitと呼ばれる高度な秘匿技術を用いたボットに感染（2006年）。

⑥米国を中心にユーザの銀行口座情報を盗むボットMetaFisherの大規模な感染が発覚(2006年)。

ボット対策プロジェクト運営開始式資料
（経済産業省、総務省他）

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

事例3：BOTの脅威（その3）

日本国内におけるボットの感染状況

- 国内におけるISP（インターネットサービスプロバイダ）ユーザのボット感染率は2～2.5%（40～50人に一人）
- ブロードバンドユーザが約2,000万契約とすると、40～50万が感染
- ボット入手実験を行った結果、一日当たり平均70種程度を入手

ボット対策プロジェクト
サイバークリーンセンターCCC

ボットはウイルスに比較して変種が多く、対策ソフトをすり抜けるボットが多数存在することから、総合的対策が必要。

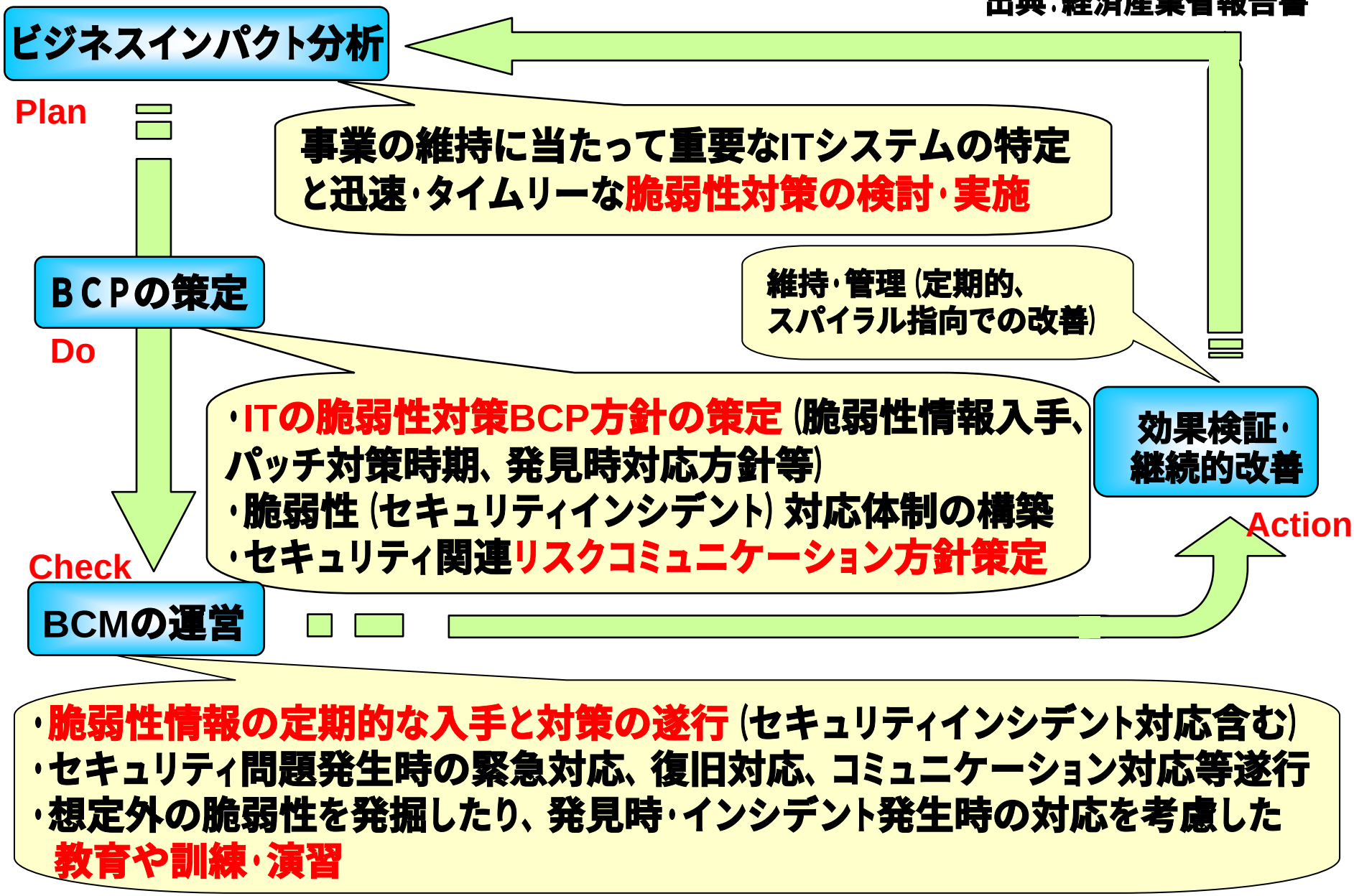
https://www.ccc.go.jp/

インターネット利用者への普及啓発活動

ボット対策プロジェクト運営開始式資料
（経済産業省、総務省他）

BCPのPDCAサイクルと脆弱性への対応

出典：経済産業省報告書



IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例1：脆弱性情報の入手と対策（その1）

脆弱性情報の入手：

脆弱性情報を公表している機関からの情報入手。

・公的なセキュリティ機関からの入手。

IPAやJPCERT/CCからの情報はJVNから入手。

➔IPAでは、届出された脆弱性に加え、日本のITシステムに関係する脆弱性情報の収集・蓄積・公開を予定。（2007年4月予定）

過去の3000件程度も蓄積・公開予定。

➔海外情報は、米国CERT/CCや英国NISCC他から入手可能。

・セキュリティ専門ベンダから脆弱性に関する情報入手（有料）。

脆弱性情報の対策（パッチ）：

迅速な対策を推進することが大切。全社内のすべてのシステムとその対応責任者や窓口担当の連絡先を登録しておくことが望ましい。推進体制の配置や対策のアウトソーシングも考慮すべき。

JPCERT/CC:Japan Computer Emergency Response Team / Coordination Center
JVN:JP Vendor Status Notes　CERT/CC:Computer Emergency Response Team/Coordination Center
NISCC:National Infrastructure Security Co-ordination Centre

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例1：脆弱性情報の入手と対策（その2）

脆弱性の存在指摘連絡時：
企業のイントラネットやWebサイトについて、問題を引き起こす脆弱性の存在をIPA他から指摘された場合には、その問題を早急に対策するための展開を進める。
このような脆弱性情報の社内展開を支援する体制を配置することが望ましい。CSIRT（Computer Security Incident Response Team）構築。
セキュリティ維持のアウトソーシングサービスを受けることも考慮。

自社で脆弱性発見時：
自社のシステムへの対策を優先して実施するのは当然であるが、同じような脆弱性が他社のシステムでも存在する可能性があるときは、IPAへの届出・相談を積極的に実施することをお願いします。

CSIRT：コンピュータ・セキュリティに関する事故が発生した場合に、実際に対応に当たる組織。
米国のCERT/CCや日本のJPCERT/CCなどが公共的なCSIRTだが、CSIRTとは企業や自治体などでのみ活動するといった、業務範囲が限られた組織といったとらえ方が多い。
CSIRT設置に当たってはどのような問題が起きる可能性があるのかを洗い出す事前調査から、障害発生時に際しての指揮命令系統の確保、外部専門機関との連絡体制の確認などを考慮する必要がある。

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例2：演習

内閣官房情報セキュリティセンター(NISC: National Information Security Center)

新たな体制の構築

1．重要インフラ横断的機能の強化

➢内閣官房のセンターを中心に重要インフラ横断的な状況把握（相互依存性解析等）を実施

2．情報共有・提供体制の強化

➢「情報共有・分析センター」（ISAC; Information Sharing & Analysis Center）等の各重要インフラ内情報共有機構の創設
➢重要インフラ横断的な情報共有の推進（「重要インフラ連絡協議会」（仮称）の設立等）
➢情報提供体制の整理・強化、情報の充実・質の向上

3．総合的演習の実施

➢想定脅威に対応した具体的脅威シナリオの類型を元に、毎年度、重要インフラ横断的な総合演習を実施

総務省：
「電気通信事業分野におけるサイバー攻撃対応演習」に係る実施計画の概要
平成18年12月1日発表。2007年2月までに演習と結果検証・評価を予定
1）重要サイトDDos攻撃対応演習
2）DNS攻撃対応演習
3）IP電話スパム攻撃対応演習

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例3：リスクコミュニケーション（その1）

日本銀行サイトのDDoS攻撃への公表（ベストプラクティス）

日本銀行では、2006年12月13日20：50にホームページで状況等について公表。
その後、適宜解決まで状況報告を継続。随時公表資料（2006年）で公表。

12月13日 日本銀行ホームページの状況等について（20：50時点）
http://www.boj.or.jp/type/release/zuiji_new/un0612a.htm
12月14日 日本銀行ホームページの状況等について（1：30時点）
12月14日 日本銀行ホームページの閲覧障害について（続報）

14日には、複数のニュースサイトで「日本銀行DDoS攻撃、現在は解消」等のメール配信されている。

メディアとの連携を意識したリスクコミュニケーションが大切。
資料という閲覧者が見つけやすいところに配置する工夫も必要。

トップページ・ワンクリックの状況提供（ベストプラクティス）

2006年12月27日台湾沖地震に伴う障害発生時、トップページに「重要なお知らせ　台湾沖地震に伴う障害の発生について（お詫び）」とワンクリックで障害状況が把握できるようにしている。

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例3：リスクコミュニケーション（その2）

日本銀行での公表状況（ベストプラクティス）

日本銀行ホームページの状況等について（20：50時点）

2006年12月13日
日本銀行

現在、日本銀行ホームページに集中的な不正アクセスがあり、閲覧が不安定な状態となっています。利用者の皆様には大変ご迷惑をおかけしております。

現在、安定的な閲覧に向けて、鋭意作業を行っておりますが、今後、仮に、日本銀行ホームページへの接続や閲覧が不安定な場合、日本銀行大阪支店ホームページに掲載されている同バックアップ・サイト（http://bkup.boj.or.jp/）において、最新の情報がご覧になれますので、そちらをご覧下さい。

照会先：情報サービス局　XX（03-ABCD-EFGH）

以　上

日本銀行ホームページの状況等について（1：30時点）

2006年12月14日
日本銀行

昨日、一時本行ホームページの閲覧が不安定になる事象が発生しましたが、現時点では閲覧可能な状態になっております。

今後、仮に、日本銀行ホームページへの接続や閲覧が困難な場合は、日本銀行大阪支店ホームページに掲載されている同バックアップ・サイト（http://bkup.boj.or.jp/）において、最新の情報がご覧になれますので、そちらをご覧下さい。

照会先：情報サービス局　XX（03-YYYY-ZZZZ）

以　上

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

BCMの適用例3：リスクコミュニケーション（その3）

日本銀行での公表状況（ベストプラクティス）

日本銀行ホームページの閲覧障害について（続報）

2006年12月14日
日本銀行

12月13日午後7時30分頃より10時頃まで、日本銀行ホームページ（http://www.boj.or.jp）に対し、海外と思われる複数の先から、集中的な不正アクセスがあったことから、同ホームページの閲覧が困難となる状態が発生しました。利用者の皆様に大変ご迷惑をおかけいたしました。深くお詫び申し上げます。

現在は、所要の措置を講じたことにより、閲覧に支障のない状態に戻っており、今後予定されている統計等の公表は、予定どおり行います。なお、万が一、再度閲覧が不安定となった場合でも、大阪支店ホームページ上のバックアップサイト（http://bkup.boj.or.jp）において、最新の情報をご覧になれますので、そちらをご覧ください。

今回の集中的な不正アクセスは、本年9月22．25日の不正アクセスと同様、日本銀行ホームページの障害を企図したものと考えられ、日本銀行としては極めて遺憾であります。今後も不正アクセスへの対応をより強化するとともに、内閣官房の情報セキュリティ関連部署や警察庁．警視庁とも連携しつつ、適切な対応を講じていく所存であります。

以　上

本件についての照会先
日本銀行　情報サービス局
XX　03-ABCD-EFGH
YY　03-JKLM-NOPQ

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

考慮すべきベストプラクティスまとめ（その1）

「セキュリティインシデント」に対する考慮項目例

適用範囲とビジネスインパクト分析：

・ソフトウエアの脆弱性を悪用した不正アクセス、コンピュータウイルス感染やWeb改ざん等より業務の停止・低下、個人情報の漏洩や情報の改ざんなどの発生により顧客・協力会社や社会から信頼を失い、経営に重大な影響を及ぼすことを想定したBCPを策定する。

・本BCPで対象とする情報システムは、たとえば、オンラインショッピングサイト。

個々の情報システムの目標復旧時間（RTO）の設定。たとえば、システム停止をしてから脆弱性対策を実施し、システム再開までの目標復旧時間を決める。4時間とか1日。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

考慮すべきベストプラクティスまとめ（その2）

BCP策定：

・社内対応体制、社外機関との連携活動方針を決める。たとえば、社内の連絡体制と各連絡先の文書化。社外機関との連携では、脆弱性情報を定期的にIPAとJPCERT/CCが共同運営するJVNから入手したり、セキュリティサービス事業者から最新インシデント情報等を入手する等の方針を決める。

・個人情報の漏えいの可能性があるときのリスクコミュニケーション方針や、Webサイトを停止するときの公表方法等の方針を決める。

・外部からのセキュリティインシデントに対する指摘をスムーズに対応するため、社内の適切なセキュリティ担当者に情報が正確に伝わるよう、社内のWeb窓口やコールセンターとの連携方法を決めておく。

・Web開発時に脆弱性を作りこまないように確認すべき項目を明確にすること、脆弱性発見時の対策方法を契約時にどう記載するかを明確にする。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

考慮すべきベストプラクティスまとめ（その3）

BCMの運用：

- 脆弱性情報の定期的な入手と計画的な対策の実施。
- 定期的なセキュリティ診断の実施（専門家への依頼も含む）。
- セキュリティインシデント発生時は、状況把握やインシデント特定とその対応を実施する。（セキュリティ問題発生時の緊急対応、復旧対応、コミュニケーション対応等遂行）
- リスクコミュニケーションにおいては、「信頼される企業」としての行動を基本とする。
- 一般従業員を含んだ、セキュリティ教育を定期的に実施し、セキュリティ上のリスク低減を図る。（セキュリティに対する企業ポリシーを徹底的に教育する。啓発教育、セキュアプログラミング教育等の実施。その際、IPAの公開資料の活用も。）
- 想定外の脆弱性を発掘したり、発見時・インシデント発生時の対応を考慮した教育や訓練・演習

効果検証・継続的改善：

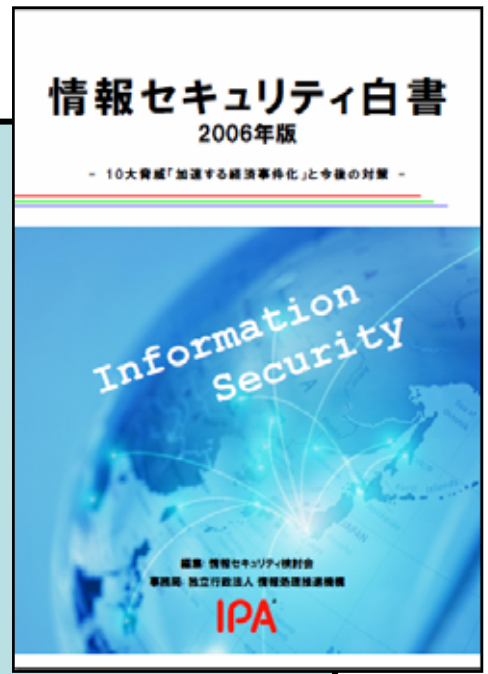
- 維持・管理（スパイラル指向での改善、できるところから対応する）

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティ白書と情報セキュリティ教本

- 社会的影響の大きさから10大脅威を列挙
- 利用者、管理者、開発者それぞれの立場での対策

情報セキュリティ白書 2006 年版 - 10 大脅威「加速する経済事件化」と今後の対策 –
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html



1. 事件化するSQLインジェクション
2. Winnyを通じたウイルス感染による情報漏洩の多発
3. 音楽CDに格納された「ルートキットに類似した機能」の事件化
4. 悪質化するフィッシング詐欺
5. 巧妙化するスパイウェア
6. 流行が続くボット
7. ウェブサイトを狙うリンクの罠
8. 情報家電、携帯機器などの組込みソフトウエアにひそむぜい弱性
9. セキュリティ製品の持つぜい弱性
10. ゼロデイ攻撃

「情報セキュリティ白書2007」、「情報セキュリティ教本」：近日発行

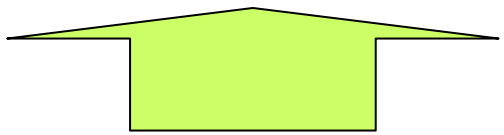
3．まとめのようなもの

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

まとめのようなもの

一緒にやっていきましょう（一人ではできない）

脆弱性（ぜいじゃくせい）
Vulnerability
2010年には10万件/年の脆弱性発見
300件/日の取り扱い！！



作り込まない
作り込ませない
情報共有と継続した対策の覚悟
(攻撃者はいつでも攻撃してきます)

Webは、社会・経営活動のプラットフォーム