

インシデント

セキュリティ侵害のリスクの現状・動向

具体的なセキュリティインシデント対応を主体に

Let's update!

2010. 1. 25

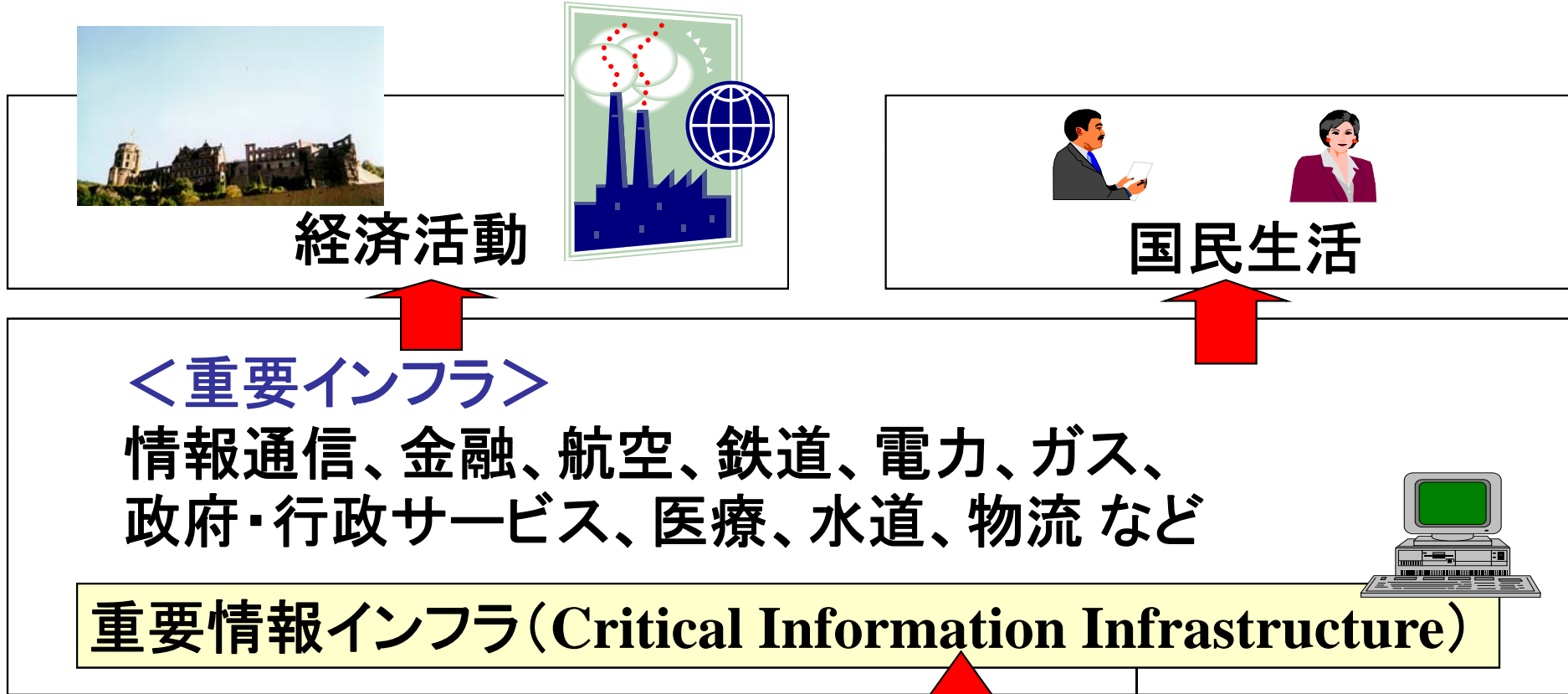
独立行政法人 情報処理推進機構

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

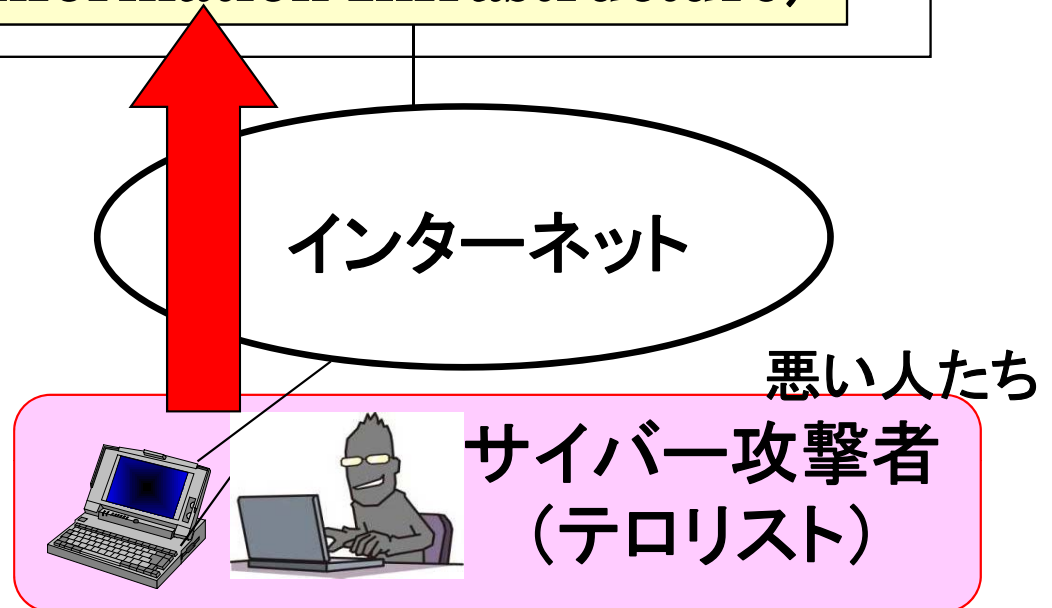
小林 偉昭 hd-koba@ipa.go.jp

サイバー攻撃(テロ)の概要



<サイバー攻撃(テロ)>

重要情報インフラに侵入し、
 データを破壊、改ざんしたり、
 重要情報インフラを機能不全
 にすること



サイバーテロ(攻撃)も映画に

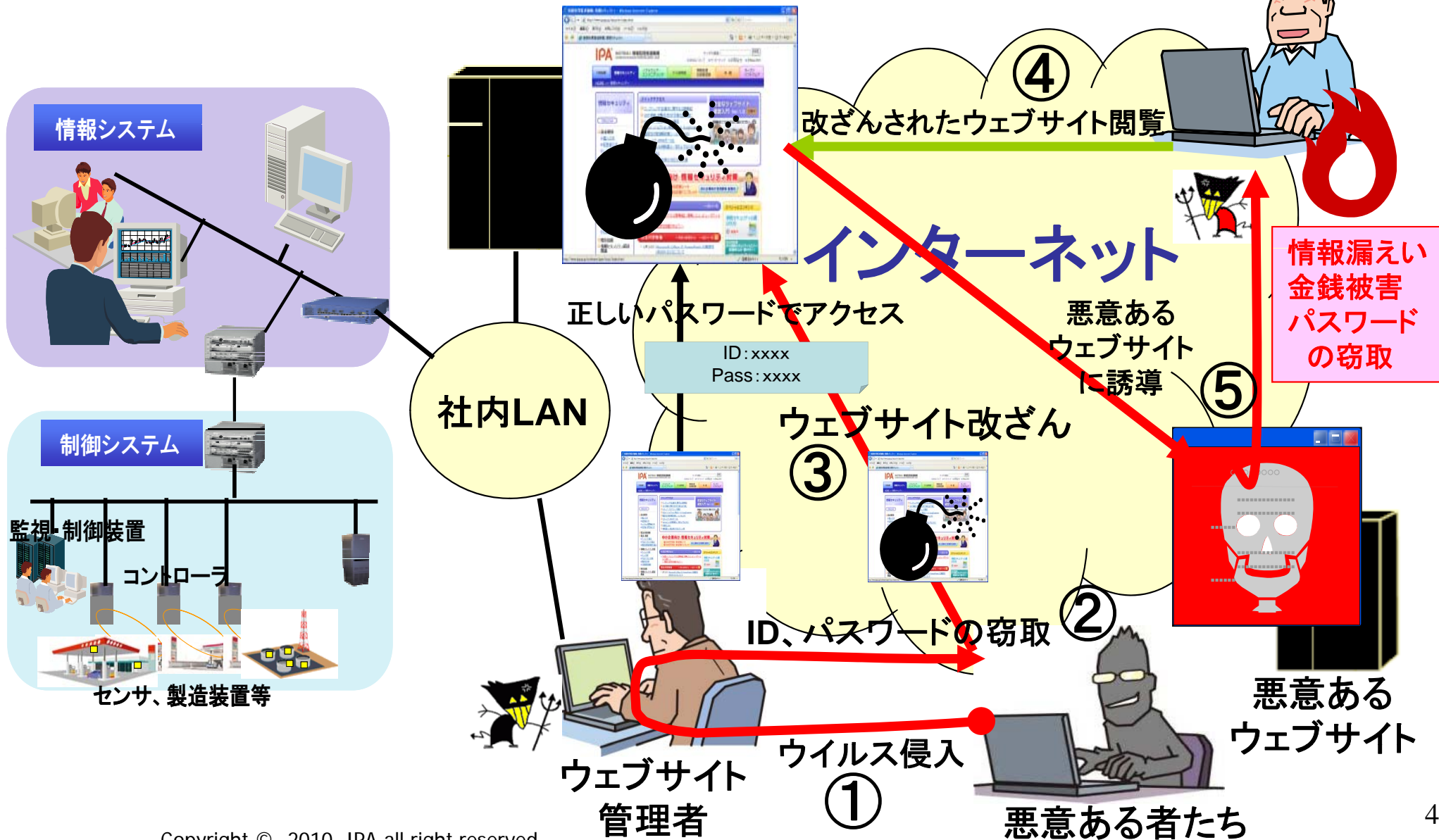
金融街の交通システム、航空管制システムやテレビ放送の制御奪取等の攻撃

<http://movies.foxjapan.com/diehard4/>

金融、鉄道関係での発生例

一般利用者

改ざんされた信頼されている企業のウェブサイト

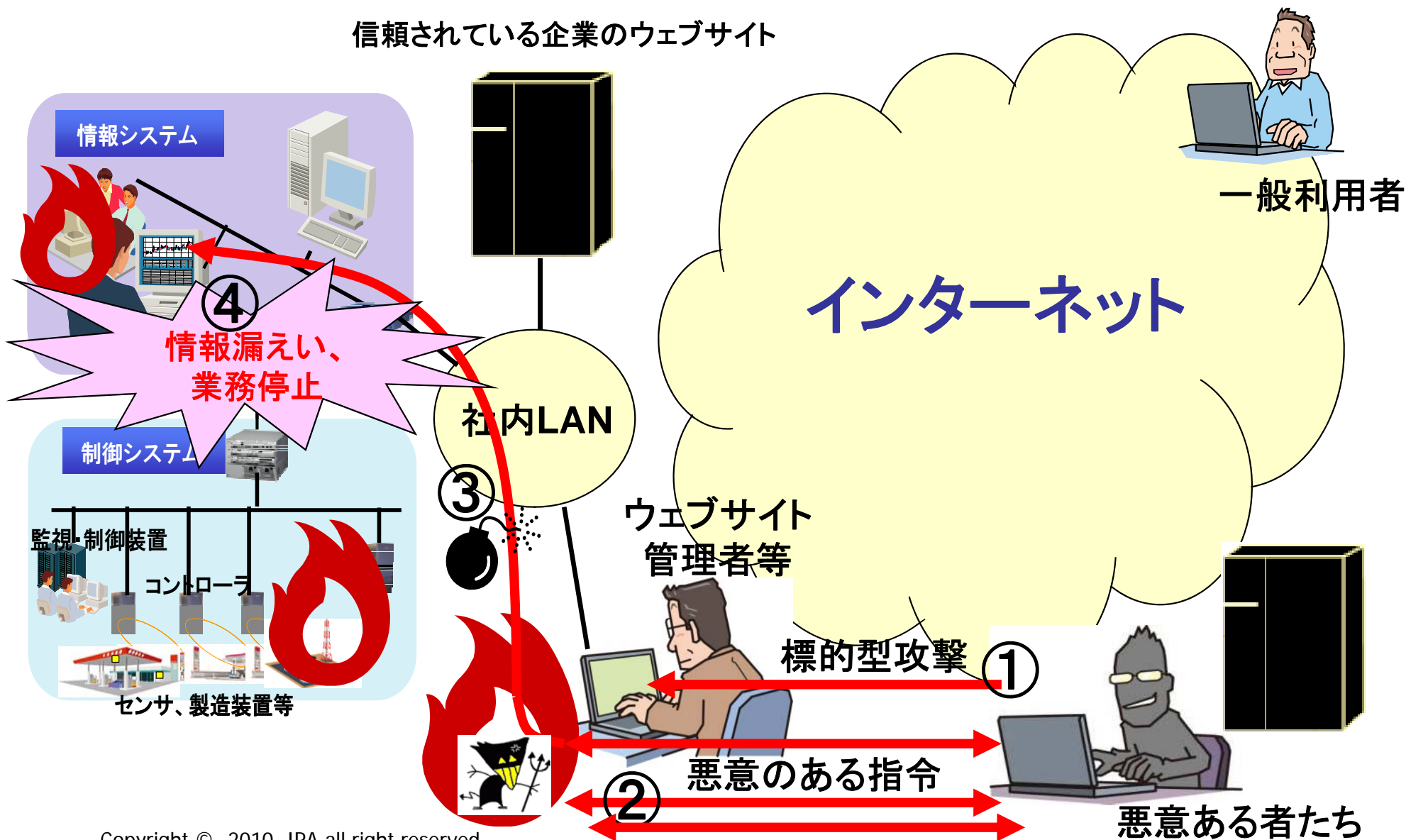


BCPは「もし起きたら」を考えた対策を

BCP: Business Continuity Plan

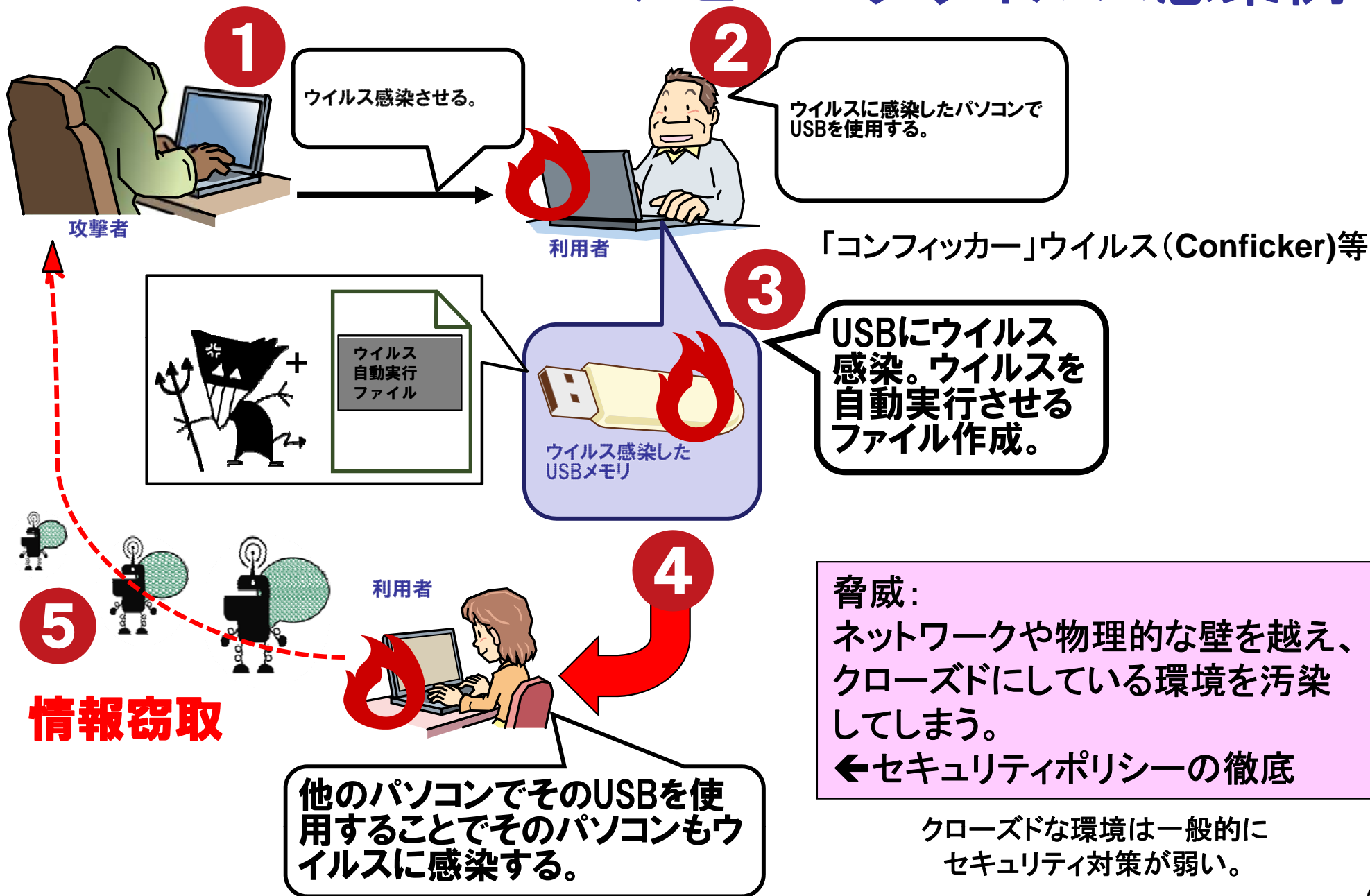
アカウント情報窃取だけでなく……悪意のある指令も……

信頼されている企業のウェブサイト

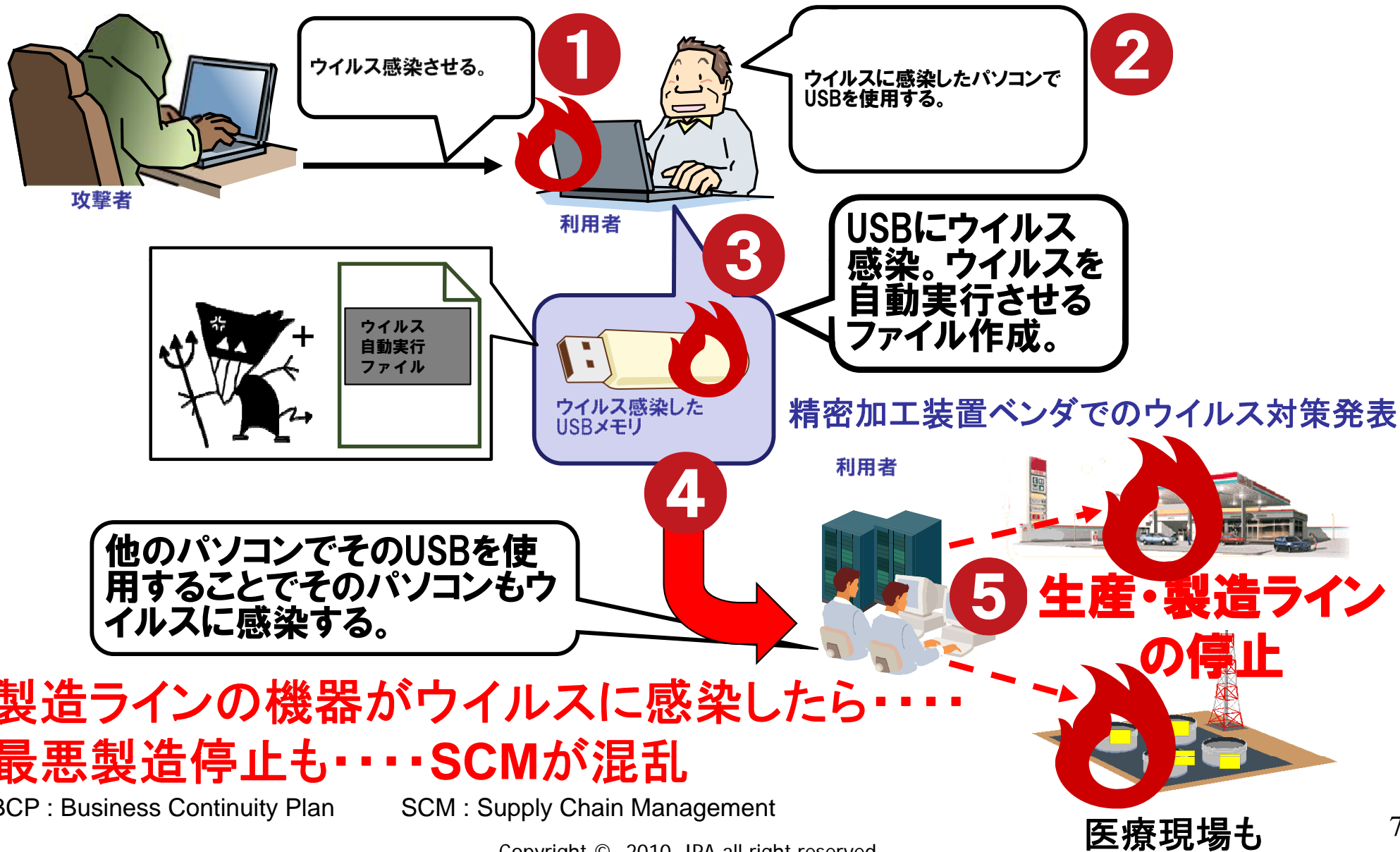


ケース3

外部メディア(USB等)での コンピュータウイルス感染例



BCPは「もし起きたら」を考えた対策を



BCP : Business Continuity Plan

SCM : Supply Chain Management

企業のセキュリティリスク例

BCMとしての対応が必要

ケース1と3 : 一般の利用者が被害者
 個人情報(銀行カード情報や医療情報等)が窃取される
 →金銭賠償、企業への信頼喪失
 改ざん情報(株価情報や政治的トピックス等)による被害
 →金銭賠償、社会混乱、企業への信頼喪失
 ボットネットとしてDDoSやスパムメールに利用される
 →社会混乱、企業への信頼喪失

重要なウェブ選別と
 多重防護対策
 * 更新PCの隔離
 (システム、物理的)
 運用外部委託先へも徹底
 (共用禁止)
 * PC内ソフト更新

ケース2と4 : **企業内の利用者、システムが被害**
 企業情報(取引、機密情報等)が窃取される
 →金銭被害、取引企業からの信頼喪失
 業務停止(オフィス業務、製造ラインなど)
 →金銭被害、取引企業からの信頼喪失
 社会インフラサービス停止、SCM混乱
 →社会混乱を引き起こす可能性

重要システム・情報選別
 と多重防護対策
 * サーバやアクセスPC
 の隔離
 (システム、物理的)
 * PC内ソフト更新

パソコンの高性能化やネットワーク帯域拡大により、パソコン利用者は分からない
 アンチウイルスソフトで検出できない、検出が遅い場合が起きている

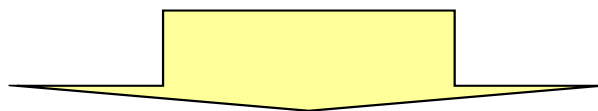
ITリスク評価の方法 — JIPDECのリスク算出式 —

<リスク値の計算式>

リスク値 = 情報資産の価値 X 脅威 X 脆弱性

<適用例>

情報資産	資産価値	脅威レベル	脆弱性レベル	リスク値
A	4	3	3	36
B	2	4	5	40



リスク値の大きい情報資産Bに対する対策を優先

リスク値のセキュリティへの適用

リスク値 = 情報資産の価値 × 脅威 × 脆弱性

情報資産の価値 : 重要システム(ウェブシステム含む)と情報の洗い出し、ビジネスインパクト分析など

脅威 : 攻撃のしやすさ、攻撃者の動機やツールの存在、対策情報の存在など

脆弱性 : 攻撃に対する弱点

参考

共通脆弱性評価システム CVSS (Common Vulnerability Scoring System)

(1) 基本評価基準 (Base Metrics)

脆弱性そのものの特性を評価する基準です

(2) 現状評価基準 (Temporal Metrics)

脆弱性の現在の深刻度を評価する基準です。

(3) 環境評価基準 (Environmental Metrics)

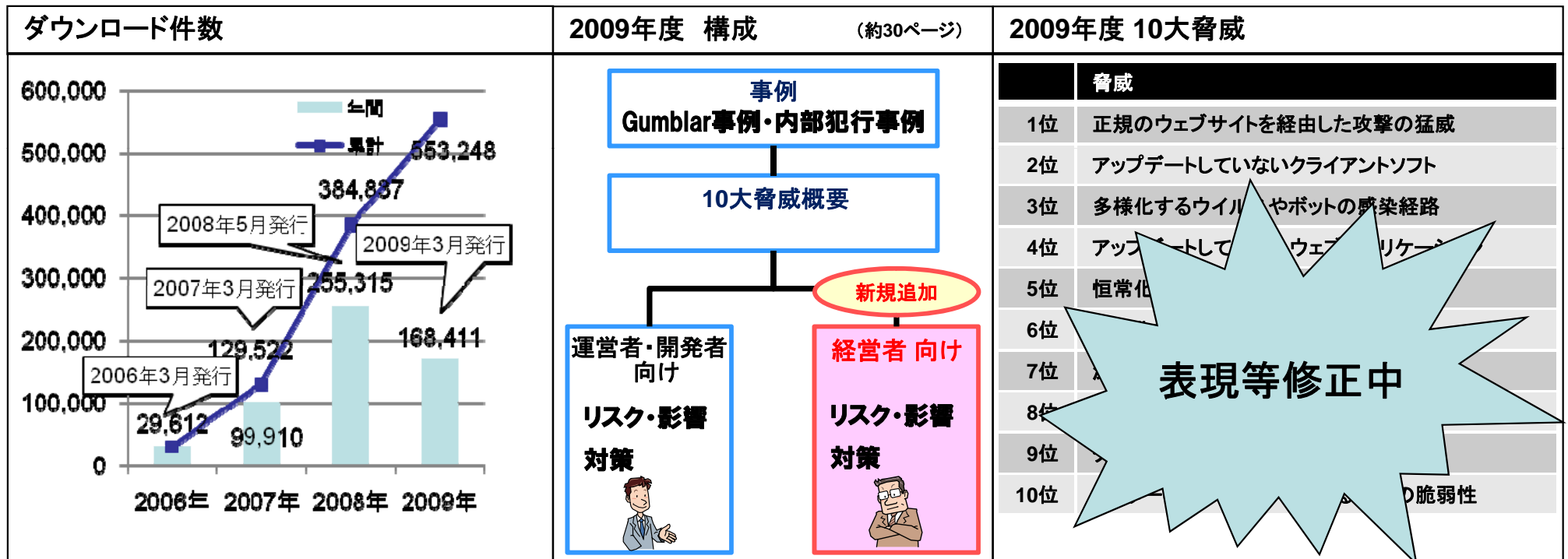
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準です。

IPA[®] 脅威に関する情報提供: 10大脅威や注意喚起

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

10大脅威 2009年度10大脅威 2010年3月に公開予定

2009年を通して注目すべき脅威をセキュリティの有識者を集めた**10大脅威執筆者会 (122名)**の意見を基に作成したドキュメント。特に**通称Gumblarの脅威を中心に記載**。開発者・運用者向けの記載に加え、**経営者向けの記載**も追加。



注意喚起 IPAセキュリティセンター : <http://www.ipa.go.jp/security/index.html>

SQLインジェクション攻撃や通称ガンブラ(Gumblar)対策等の注意喚起: 30件ほど
 JVNに登録した脆弱性対策情報の公開: 70件ほど

脆弱性対策推進:バージョンチェッカ等提供 アップデートを! 中国でのGoogle事件は!!

脆弱性対策情報

JVN/
JVNiPedia

7600件
以上

MyJVN

Shockwave Player 予定

- 2009/11/30 MyJVN バージョンチェッカ提供
- 2009/12/21 MyJVN セキュリティ設定チェッカ提供
- 2009/12/24 改ざんされたウェブサイトからのウイルス感染に関する注意喚起

<http://jvndb.jvn.jp/apis/myjvn/index.html>

JVN iPedia

- 2009/6/18 利用者向け機能強化
 - ・検索機能強化(類義語検索など)
- 2009/12/28 **登録件数累計 7,646件**(年間1,876件増)

<http://jvndb.jvn.jp/>

国際連携

- 2010/1/8 CVE互換認定取得
- 2010/1/19 CVSS の計算ソフトウェアを多言語化(7カ国語化対応※)

月間アクセス100万件突破

(2009年12月)

Internet Explorerの古いバージョンが...

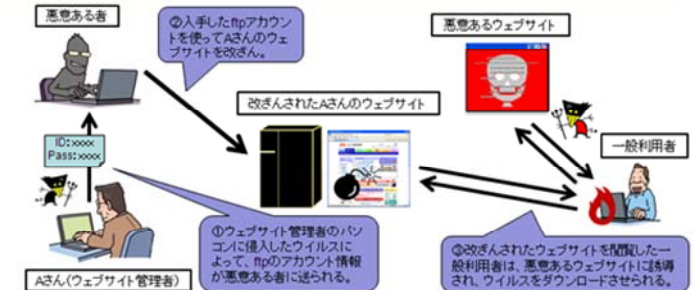
MyJVNバージョンチェッカのURLが掲載された一般紙の記事が、インターネットポータルサイト(Yahooなど)で紹介されたことにより、アクセス数が急増している(2010年1月)

1月6日 毎日.jp掲載

1月11日 産経ニュース掲載

1月18日 YOMIURI ONLINE掲載

ウェブサイト管理者へ:ウェブサイト改ざんに関する注意喚起
一般利用者へ:改ざんされたウェブサイトからのウイルス感染に関する注意喚起

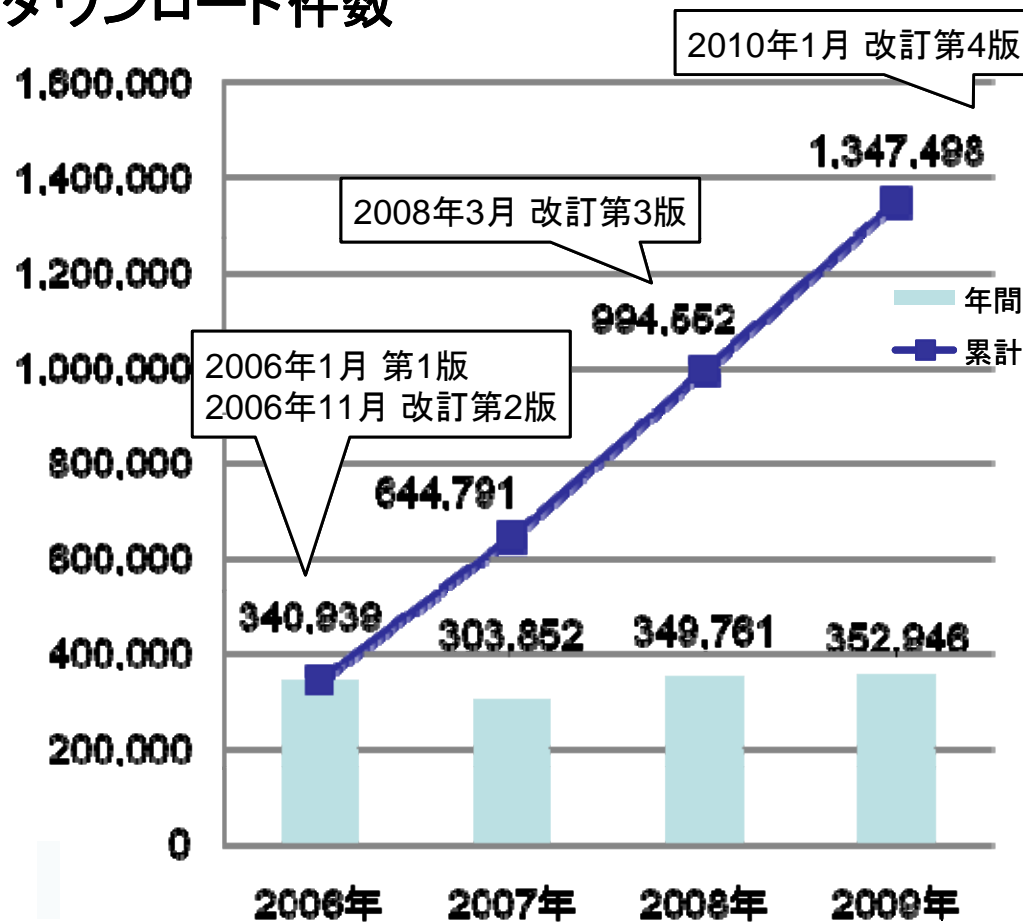


脆弱性を作りこまないために

「安全なウェブサイトの作り方」、「安全なSQLの呼び出し方」

ウェブサイトの脆弱性を作りこまないための、**具体的な対策**を説明したドキュメント。
届出に基づいた説明を展開。対策を「根本的解決」と「保険的対策」に分けた取組みを可能に。

ダウンロード件数



累計: 134万件 (2006年1月～)



「安全なウェブサイトの作り方 改訂第4版」

発行日: 2010年1月20日
 ページ数: 92ページ

※ 改訂第3版 (2008年6月発行、76ページ) に、失敗例4種類と、WAFの説明を追加。

<http://www.ipa.go.jp/security/vuln/websecurity.html>



別冊「安全なSQLの呼び出し方」

発行日: 2010年2月(予定)
 ページ数: 32ページ(予定)

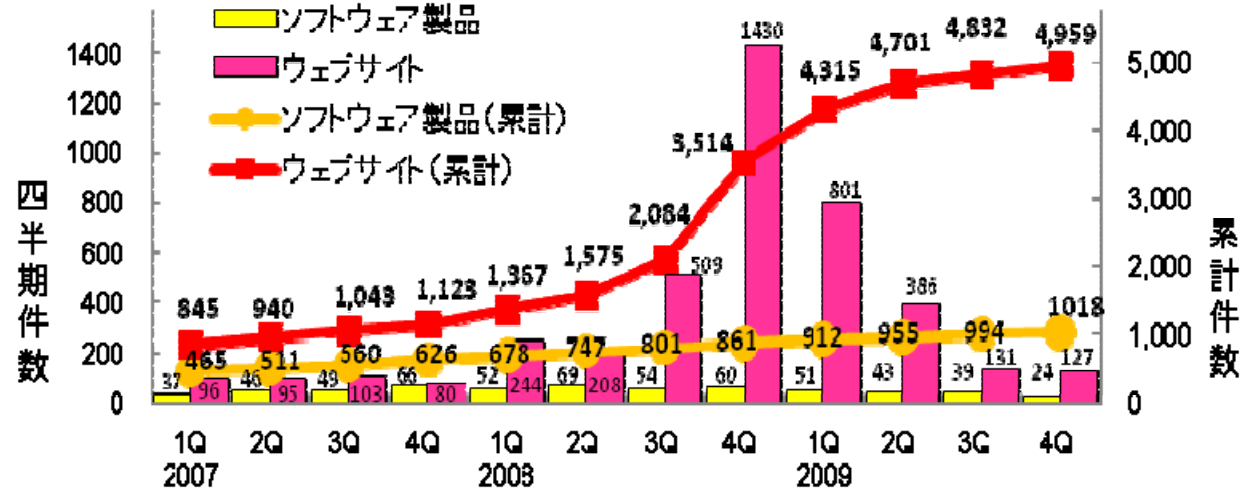
※ 「安全なウェブサイトの作り方」のSQL関連部分を具体化し、新規に作成。

脆弱性の届出状況と公表した脆弱性対策情報の傾向

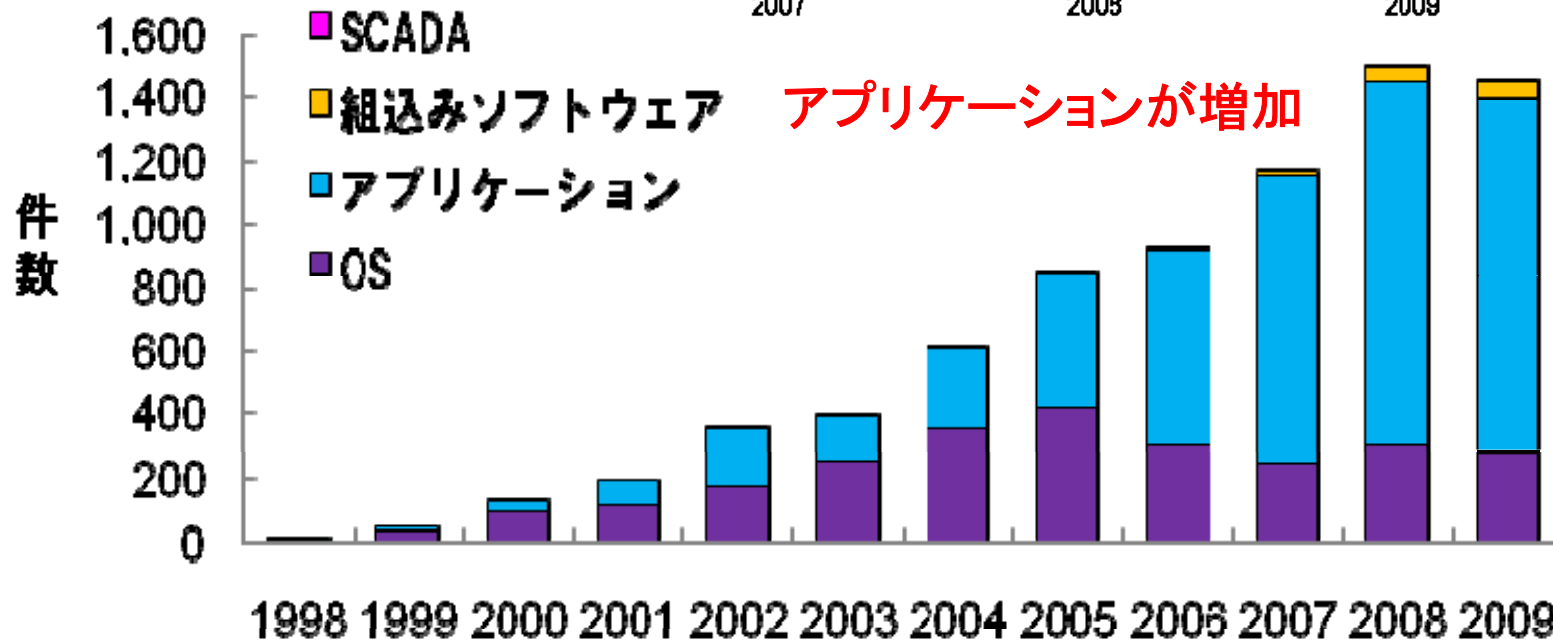
脆弱性の届出状況

届出件数6,000件突破！

<http://www.ipa.go.jp/security/vuln/report/vuln2009q4.html>



公表した脆弱性対策情報の傾向



アプリケーションが増加

SCADA関連
少しずつ増加
2008年6件
2009年9件
合計15件公開

1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009
<http://www.ipa.go.jp/security/vuln/report/JVNiPedia2009q4.html>

脆弱性対策情報を公表した製品の種類の公開年別推移

ご清聴ありがとうございました。

「重要インフラ制御システムの脆弱性低減
と普及施策に関する調査」報告書
2010年4月 IPAウェブサイトで公開予定

Let's update!

IPA セキュリティセンター

参考資料

ITの脆弱性へのBCM適用例

ビジネスインパクト分析

Plan

事業の維持に当たって重要なITシステムの特定と迅速・タイムリーな脆弱性対策の検討・実施

BCPの策定

Do

維持・管理(定期的、スパイラル指向での改善)

- ・ITの脆弱性対策BCP方針の策定(脆弱性情報入手、パッチ対策時期、発見時対応方針等)
- ・脆弱性(セキュリティインシデント)対応体制の構築
- ・セキュリティ関連リスクコミュニケーション方針策定

効果検証・継続的改善

Check

BCMの運営

Action

- ・脆弱性情報の定期的な入手と対策の遂行(セキュリティインシデント対応含む)
- ・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
- ・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

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。

7600件程度も蓄積・公開。JVNiPedia

→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

Copyright © 2010, IPA all right reserved.

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システムの確保、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。

「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:

- ・ソフトウェ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。

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入手する等の方針を決める。
- ・個人情報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。

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 to 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)²²