IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

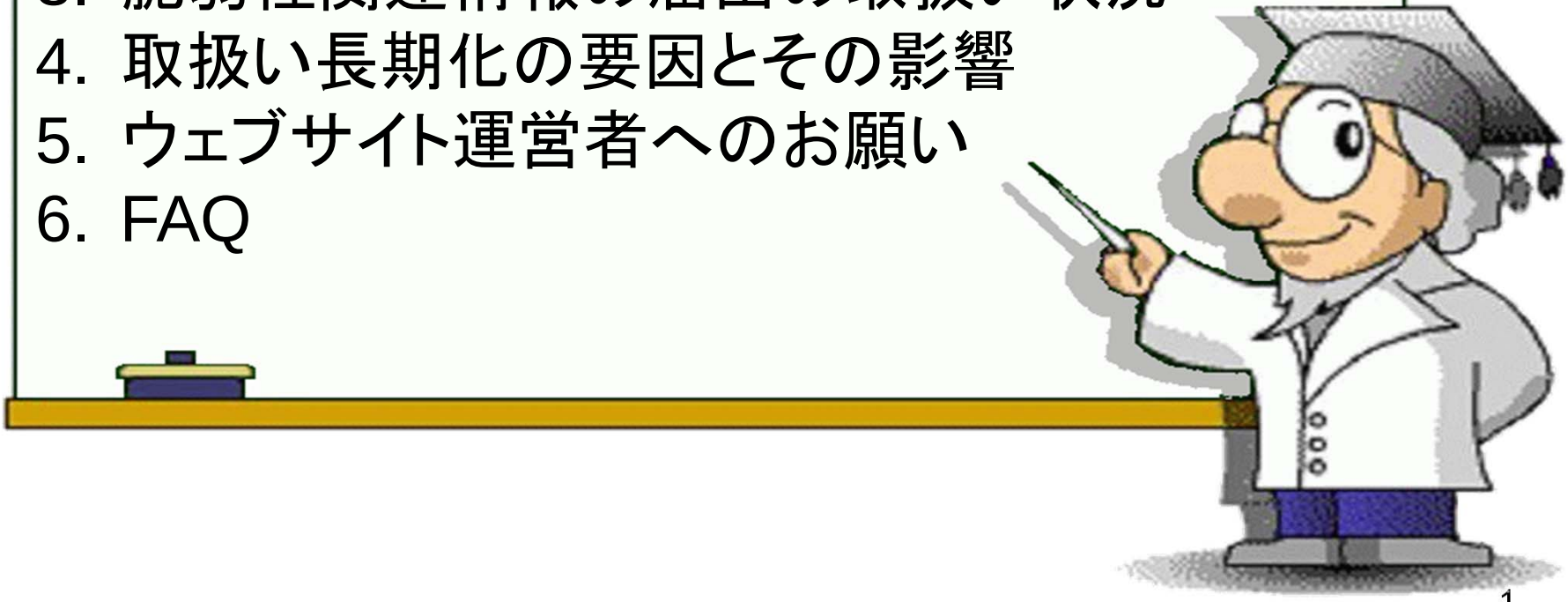
1. IPAの取り組みから分かる ウェブサイトの脆弱性対策の実情

独立行政法人 情報処理推進機構（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

2010年8月6日公開

目次

1. 脆弱性を突いた攻撃の実情
2. 「情報セキュリティ早期警戒パートナーシップ」とは？
3. 脆弱性関連情報の届出の取扱い状況
4. 取扱い長期化の要因とその影響
5. ウェブサイト運営者へのお願い
6. FAQ



1. 脆弱性を突いた攻撃の実情

1-1. そもそも「脆弱性」ってなに？

- **脆弱性（ぜいじゃくせい）とは？**

  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）

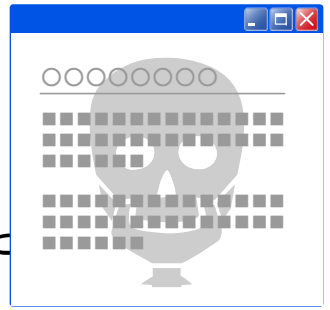
- **脆弱性を悪用されると、どうなる？**

  問題箇所を巧みに悪用し、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）

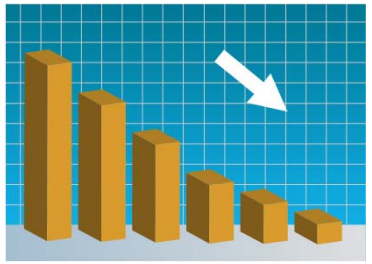
1. 脆弱性を突いた攻撃の実情

1-2. 実際の被害事例

事例①「価格情報提供サイト」

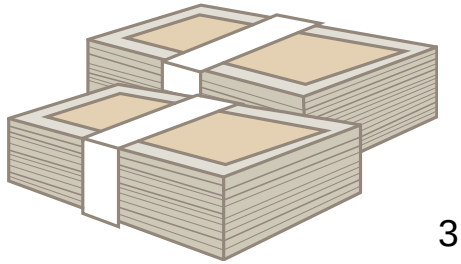


- 2005年5月、ウェブサイトに不正なプログラムが仕掛けられ、閲覧したユーザが**ウイルスに感染**したという事を発表。
- ウェブサイトのプログラムを直すそばから何者かにより改ざんされていった。その後攻撃の頻度が急増し**サイトを閉鎖**。（10日間の閉鎖）
- 登録ユーザのメールアドレス2万2511件漏えい。
- 5月の月間PVは、前月比で約4割減。
- **取引業者への影響大**。



事例②「音響機器・楽器通販サイト」

- 2008年4月、**サイバー攻撃**により顧客情報が**10万件弱流出した**可能性がある事を発表。
- クレジットカード情報が不正利用され、2008年3月にカード会社が検知し判明。
- セキュリティ会社の調査により、2006年6月頃に最初の不正侵入があった事が判明。
- 会員**12万2884人**に**1000円**を次回購入時割引。
- セキュリティ会社への作業依頼とサーバ交換等で**6,000万円強の費用**をかけた対策を行った。

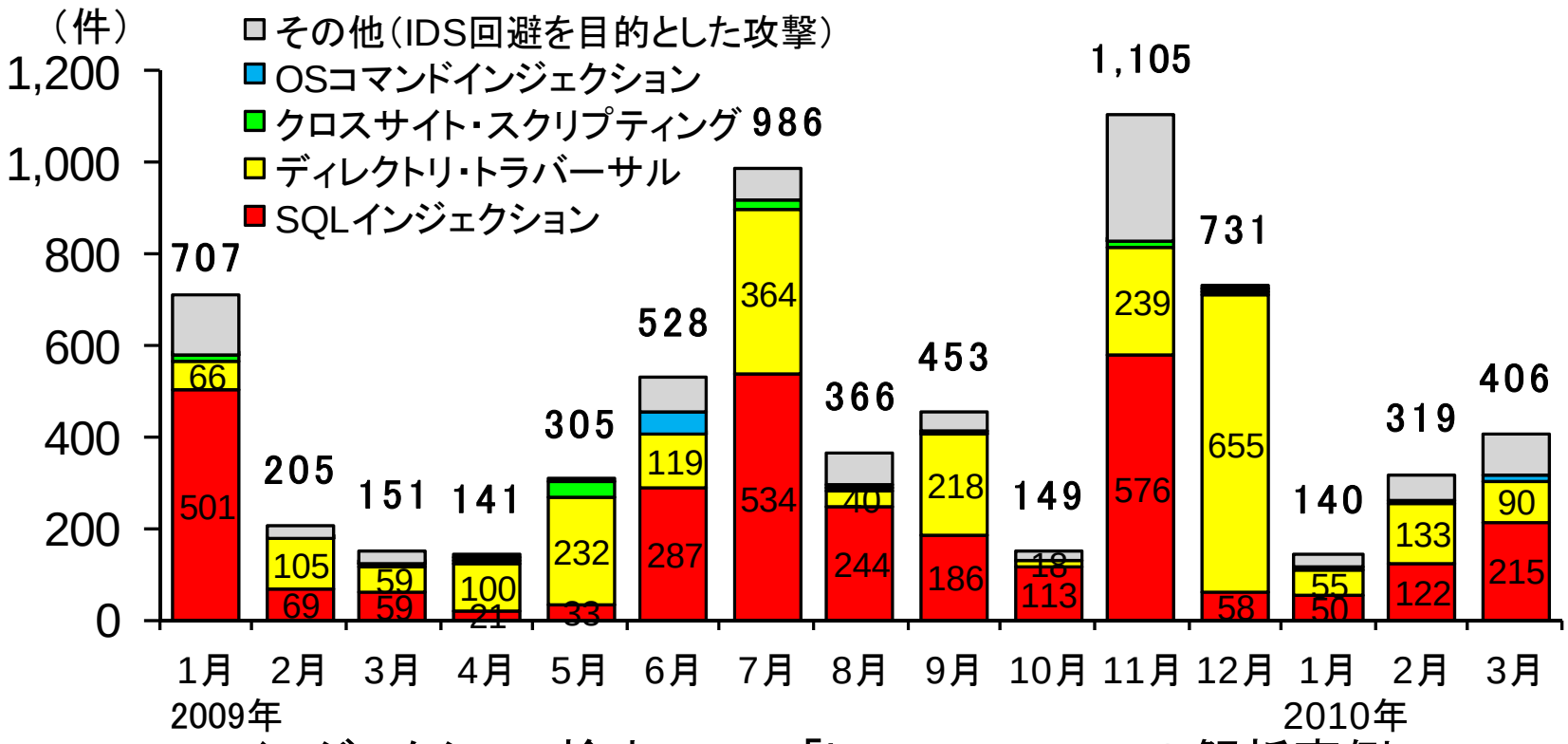


1. 脆弱性を突いた攻撃の実情

1-3. IPA のウェブサイトへの攻撃

ウェブサイトを狙った攻撃があったと思われる件数

解析対象のウェブサイト：JVN iPedia（脆弱性対策情報データベース）
解析したウェブサーバのアクセスログの期間：2009年1月～2010年3月
攻撃があったと思われる件数：平均14.7件／日、攻撃が成功した可能性の高い件数：0件



SQLインジェクション検出ツール「iLogScanner」の解析事例

2.「情報セキュリティ早期警戒パートナーシップ」とは？

2-1. 成り立ち

問題意識

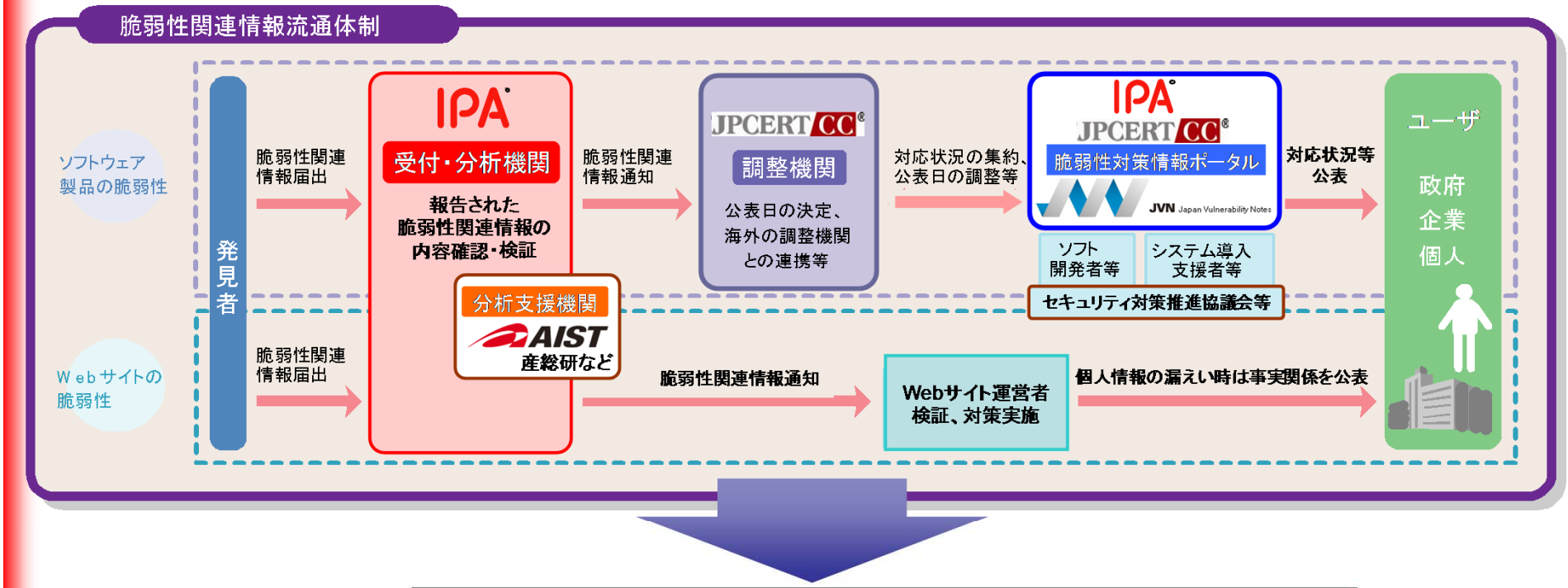
- 近年、脆弱性がコンピュータ不正アクセスやコンピュータウイルス等の攻撃に悪用されるケースが増加。
- 本来、適切に共有され対策が策定されるべき脆弱性の情報が、適切に扱われず放置、対策がない段階で暴露されることにより、大きな被害をもたらす危険性がある。さらに、脆弱性の公表から攻撃方法の出現までの期間が短縮している。
- 発見した脆弱性に関する情報の取扱いについて、日本国内の指針やガイドラインが存在しておらず、このことが報告の遅れや被害の拡大の一因となっていたことは否めない。

関係者（発見者、製品開発者、ウェブサイト運営者など）の脆弱性関連情報に対する適切な行動を促すべく、それぞれの果たすべき役割や望ましい行動基準を明示した制度（公的なルール）を導入する必要がある。

2.「情報セキュリティ早期警戒パートナーシップ」とは？

2-2. 脆弱性関連情報流通体制

2004年7月に経済産業省が「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）を公示し、「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」に則り運用を行っている。



【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不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
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

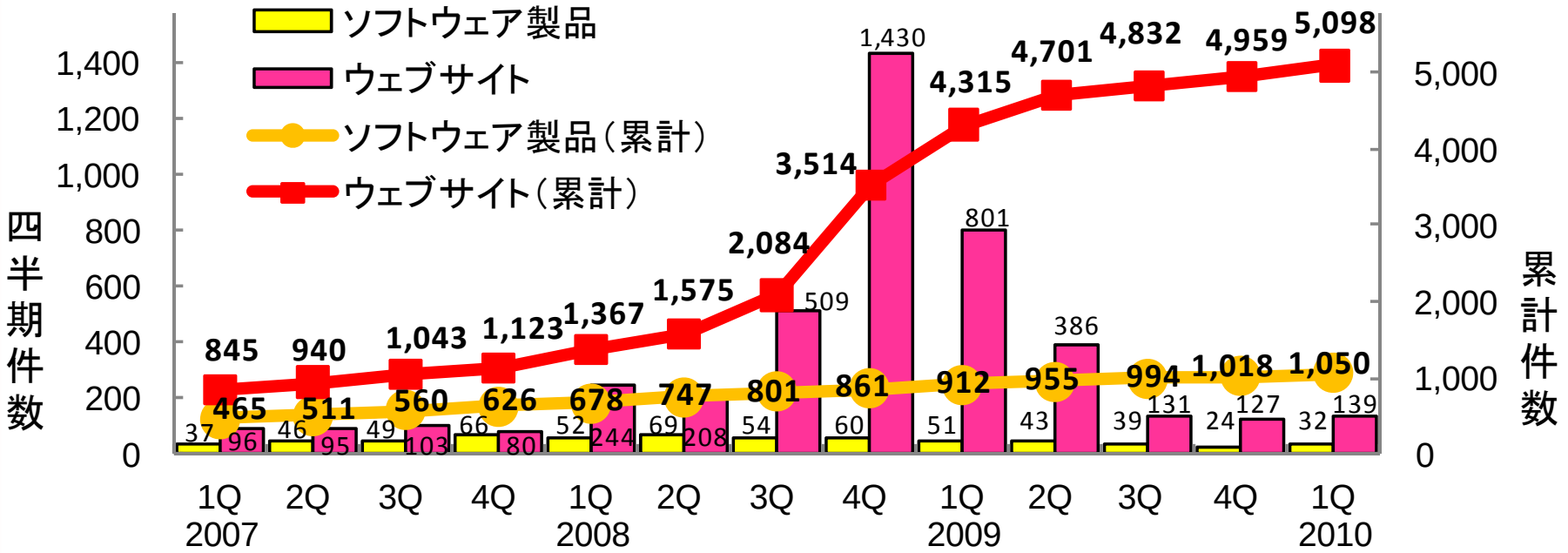
ソフトウエア等脆弱性関連情報取扱基準（http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf ）
情報セキュリティ早期警戒パートナーシップガイドライン（ http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf ）

3. 脆弱性関連情報の届出の取扱い状況

3-1. 届出状況

脆弱性関連情報の届出状況
http://www.ipa.go.jp/security/vuln/report/press.html

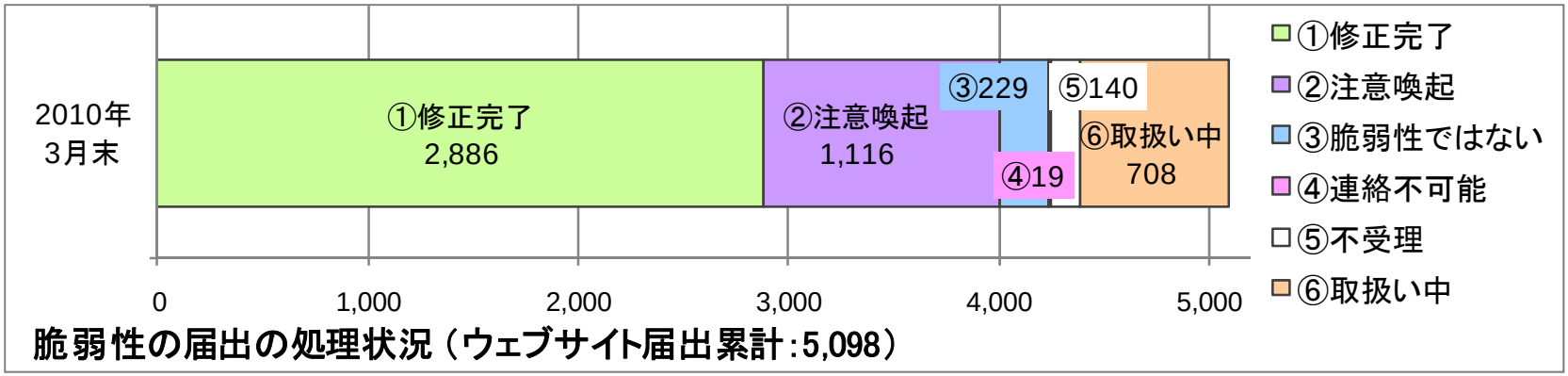
IPA へ届出される脆弱性は「氷山の一角」
世の中に潜在している脆弱性の一部である！



脆弱性関連情報の届出件数の四半期別推移

3. 脆弱性関連情報の届出の取扱い状況

3-2. 処理状況



脆弱性の届出の処理状況（ウェブサイト届出累計：5,098）

- 「①修正完了」のうち、**7 割は 3 ヶ月以内に修正を実施**している。
- 「②注意喚起」は、IPAによる注意喚起で広く対策を促した後、処理を取りやめたもの。製品のバージョンUP情報を見落としがちなため、ウェブサイト運営者は**古いバージョンのソフトウェアを利用していないか再度確認を！！**
- 「④連絡不可能」は、**ウェブサイト運営者へ連絡が取れず、処理を取りやめた**もの。

～②注意喚起について～

「EC- CUBE」の古いバージョンを利用しているウェブサイトへの注意喚起（http://www.ipa.go.jp/security/vuln/documents/2009/200907_ec-cube.html ）
「Namazu」の古いバージョンを利用しているウェブサイトへの注意喚起（http://www.ipa.go.jp/security/vuln/documents/2009/200908_namazu.html ）
「OpenSSL」の古いバージョンを利用しているウェブサイトへの注意喚起（http://www.ipa.go.jp/security/vuln/documents/2009/200909_openssl.html ）
ウェブサイトで利用されているDNSサーバの既知の脆弱性への注意喚起（http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.html）

3. 脆弱性関連情報の届出の取扱い状況

3-3. 取扱いの長期化

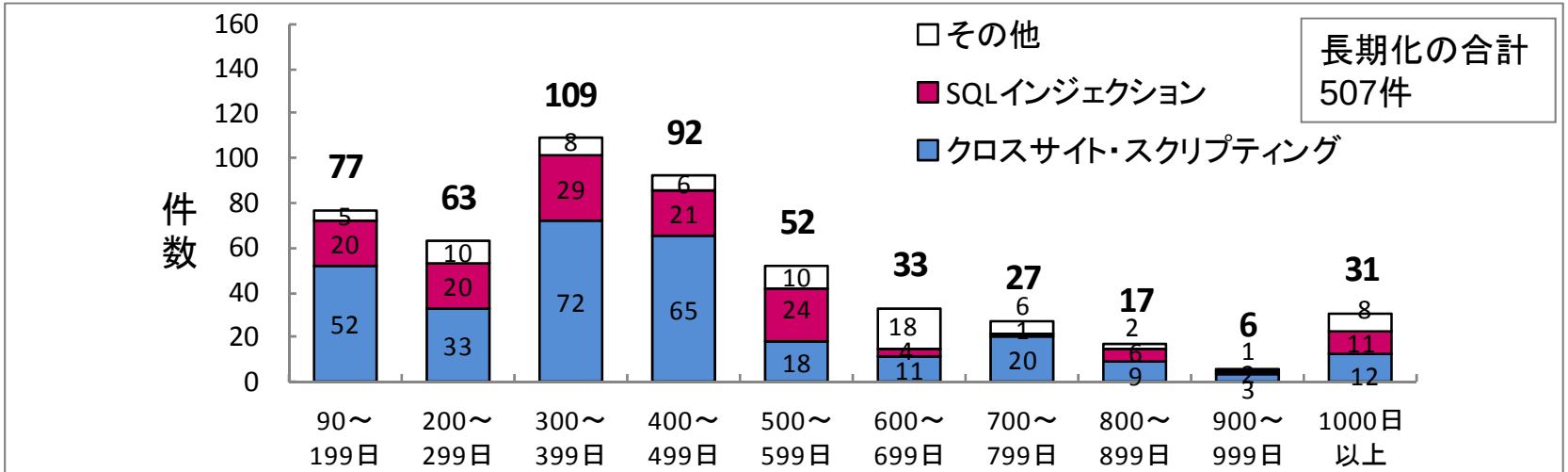


図11. 取扱いが長期化（90日以上経過）している未修正のウェブサイトの経過日数と脆弱性の種類

- 取扱い中の案件（708件）のうち、
  取扱いが長期化しているウェブサイトは507件もある。
- SQL インジェクション等の
  脅威が大きい脆弱性についても、長期化している。

4. 取扱い長期化の要因とその影響

4-1. 対策に時間を要す要因と対策

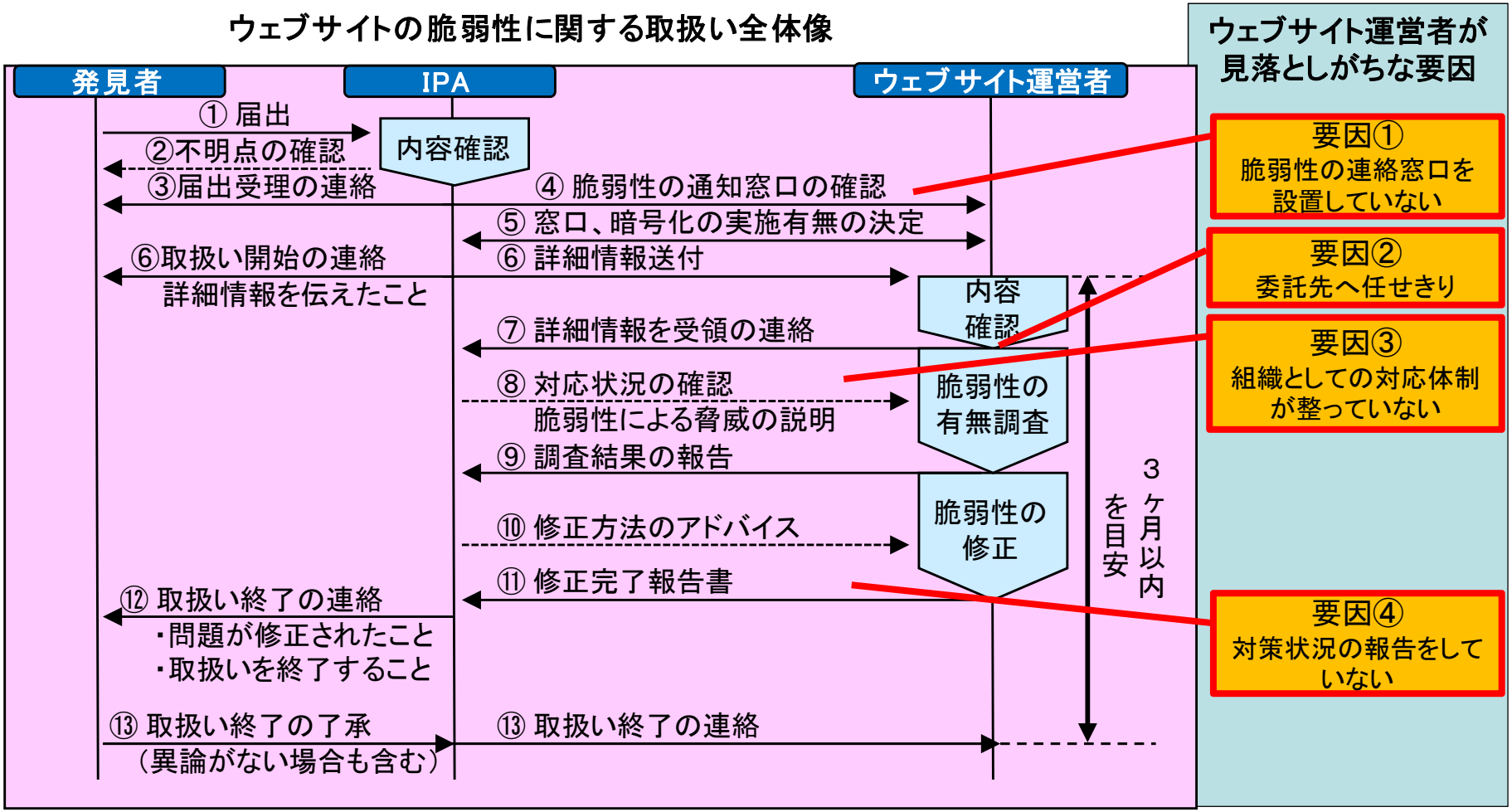
脆弱性対策および修正のための<u>予算がない。</u>このため、来年度に予算を組んで対応するしかない。

<u>修正方法が分からない。</u>
技術的に難しい問題のため検討や修正に時間を要するため、すぐには対応できない。

対策に時間を要する場合は、<u>被害を軽減するための対策</u>を実施しましょう！

4. 取扱い長期化の要因とその影響

4-2. 見落としがちな要因



脆弱性関連情報の取扱いプロセス（http://www.ipa.go.jp/security/vuln/report/process.html）

4-3. 要因とその影響

①脆弱性の連絡窓口を設置していない

- 脆弱性の発見者やIPAがウェブサイト運営者へ脆弱性情報が連絡できず、結果的にウェブサイト運営者が認識していない脆弱性が長期間放置されることになる。

②委託会社へ任せきり

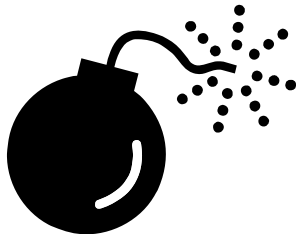
- 委託先が対応していると認識していても、実際は・・・。
- 委託先が「問題ない」と言ったため対応しなかったが、実は・・・
- 被害が発生した場合の責任は、委託先ではなく、運営者に降りかかってくる。

③組織として対応体制が整っていない

- 担当者が辞職してしまい、対応状況が把握できない。
- 始めから調査のやり直しや、そもそも対策出来ない場合も・・・。

④対策状況の報告をしていない

- 発見者はウェブサイトの利用者のため、ウェブサイトへの風評被害。



脆弱性が悪用された場合、被害はウェブサイト運営者だけではなく利用者にも及ぶ。さらに、脆弱性の指摘や届出があったにも関わらず、脆弱性を未修正のまま長期間放置していた場合、最終的には組織の社会的信頼が低下。

5. ウェブサイト運営者へのお願い

①連絡窓口を設ける

- ウェブサイト上にメールフォームや連絡先のメールアドレスを明記する。
- 脆弱性関連情報には、何処にどのような問題があるか具体的に記載されているため、第三者へ渡ると悪用される恐れがある。この為、連絡内容が公表されてしまう**BBSやTwitterなどは不可**。

②ウェブサイト運営者が主体の対応を！

- ウェブサイト運営者は、脆弱性の技術的な仕組みを理解する必要はなく、脆弱性により発生する被害とその影響を理解する。
- ウェブサイト運営者は、委託先の脆弱性修正の対応状況をきちんと把握する。

③脆弱性対応の体制を整備する

- 対応の責任者を明確にする。
- 組織として対応フローを確立する。

大企業の場合、将来的には
CSIRT「コンピュータ・セキュリティ・インシデント・レスポンス・チーム」の設置を検討すると良いでしょう！

④対応状況の報告を行う

- 対策に時間を要する場合は、対応時期の目処を報告する。
- 「対策しない」と判断した場合は、その旨と理由を報告する。

6. FAQ

Q
実際に自分のウェブサイトに対して、脆弱性の届出や指摘があった場合、どのように対応したら良いか？

A
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
を活用しましょう！

「早期警戒パートナーシップ」でよくある質問と回答については、下記を参照ください。
脆弱性関連情報の届出関連 FAQ（http://www.ipa.go.jp/security/vuln/faq.html）