プレスリリース
2008 年 10 月 14 日
独立行政法人 情報処理推進機構
有限責任中間法人 JPCERT コーディネーションセンター

ソフトウェア等の脆弱性関連情報に関する届出状況 [2008 年第 3 四半期(7 月～9 月)]

独立行政法人情報処理推進機構（略称：IPA、理事長：西垣 浩司）および有限責任中間法人 JPCERT コーディネーションセンター（略称：JPCERT/CC、代表理事：歌代 和正）は、2008 年第 3 四半期（7 月～9 月）の脆弱性関連情報の届出状況[1]をまとめました。

2008 年第 3 四半期（2008 年 7 月 1 日から 9 月 30 日まで）の IPA への脆弱性関連情報の届出件数は、ソフトウェア製品に関するもの **55** 件、ウェブアプリケーション（ウェブサイト）に関するもの **509** 件、合計 **564** 件でした。

届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの **802** 件、ウェブサイトに関するもの **2,084** 件、合計 **2,886** 件で、ウェブサイトに関する届出が全体の約 4 分の 3 を占めています（表 1）。

表 1. 2008 年第 3 四半期の届出件数

分類	届出件数	累計件数
ソフトウェア製品	**55** 件	**802** 件
ウェブサイト	**509** 件	**2,084** 件
計	**564** 件	**2,886** 件

届出が年々増加しており、届出受付開始（2004 年 7 月 8 日）から各四半期末までの業務日 1 日あたりの届出件数が、今四半期で **2.79** 件となりました（図 1）。

2008 年第 3 四半期はウェブサイトの脆弱性の届出が 509 件で、届出件数が突出して激増しました。これは、2008 年 8 月から DNS キャッシュポイズニングの脆弱性の届出が激増しているためです。全てのウェブサイト運営者は早急な調査と対策実施が必要です。詳細は P.5 の 3.2 節 3.3 節を参照下さい。

就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

2005/1Q	2006/1Q	2007/1Q	2007/2Q	2007/3Q	2007/4Q	2008/1Q	2008/2Q	2008/3Q
1.45	1.61	1.95	1.98	2.03	2.05	2.24	2.38	2.79

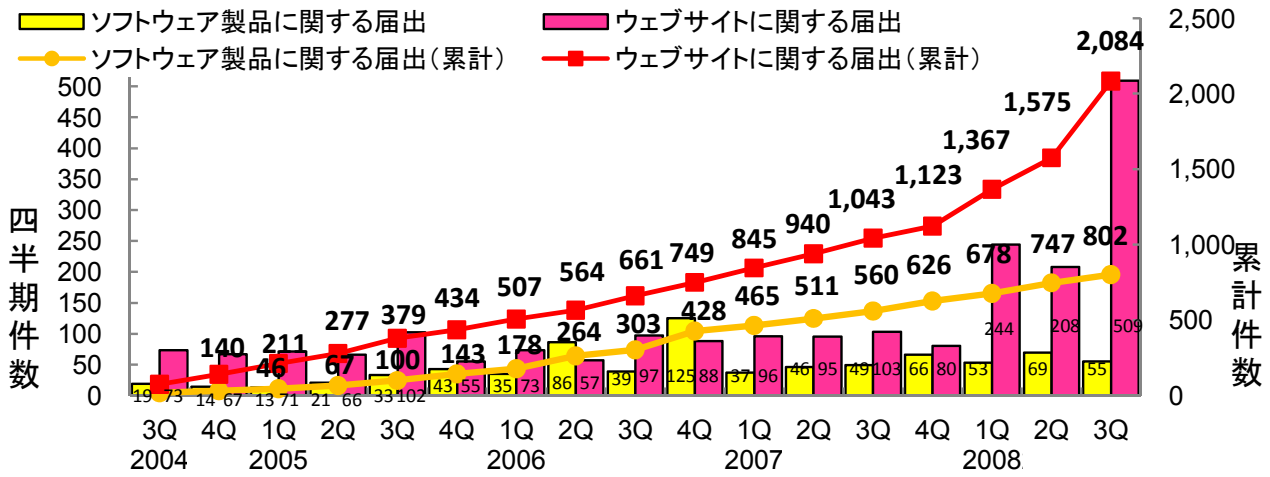


図1.脆弱性関連情報の届出件数の四半期別推移

[1] ソフトウェア等の脆弱性関連情報に関する届出制度：経済産業省告示に基づき、2004 年 7 月より開始しました。IPA は届出受付・分析、JPCERT/CC は国内の製品開発者などの関連組織との調整を行っています。

1.脆弱性の取扱い概況

2008 年第 3 四半期は、ソフトウェア製品に関しては **37** 件の取扱いが終了[2]しましたが、届出が **55** 件あったため、取扱い中は **18** 件増加して累計 **337** 件となりました。ウェブサイトに関しては **161** 件の取扱いが終了[3]しましたが、届出が **509** 件あったため、取扱い中が **348** 件増加して累計 **698** 件となりました。

図 2 は、ソフトウェア製品に関して各四半期に届出のあったものの現在の取扱い状況です。例えば、2006 年第 3 四半期に届出のあったものは、23 件の取扱いを終了しましたが 16 件は取扱い中です。また、2007 年第 3 四半期に届出のあったものは、26 件の取扱いを終了しましたが 23 件は取扱い中です。

このように、**ソフトウェア製品に関しては、2006 年に届出られたものでも、今だ 36%が取扱い中のままです。2007 年に届出られたものは、47%が取扱い中のままです。ソフトウェア製品開発者は、脆弱性を攻撃された場合の顧客システムへの影響の重大さを認識し、早期に対策を講じる必要があります。**

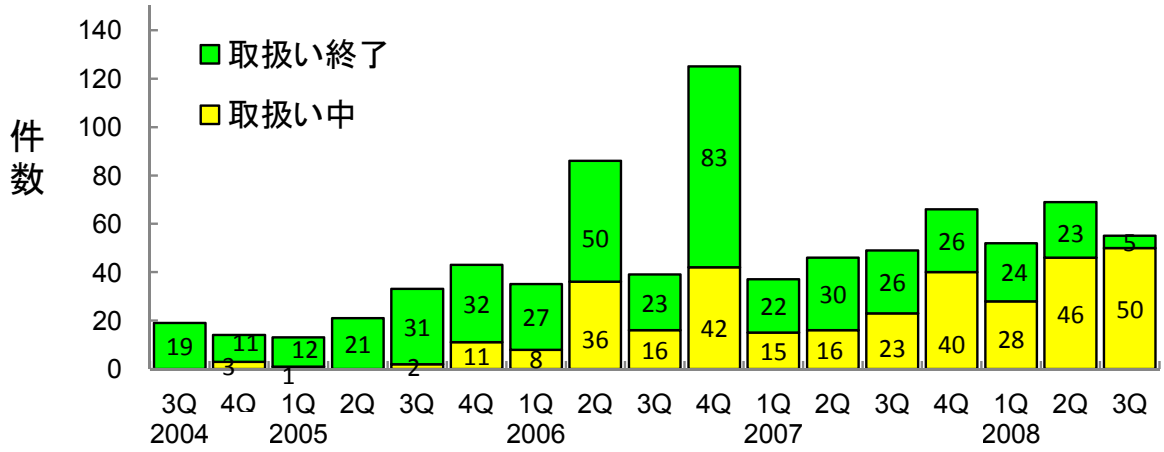


図2. ソフトウェア製品に関して各四半期に届出のあったものの現在の状況

ウェブサイトに関しては、2007 年に届出られたものの 20%が取扱い中のままです（図 3）。ウェブサイト運営者は、脆弱性を攻撃された場合の重大さを認識し、早期に対策を講じる必要があります。

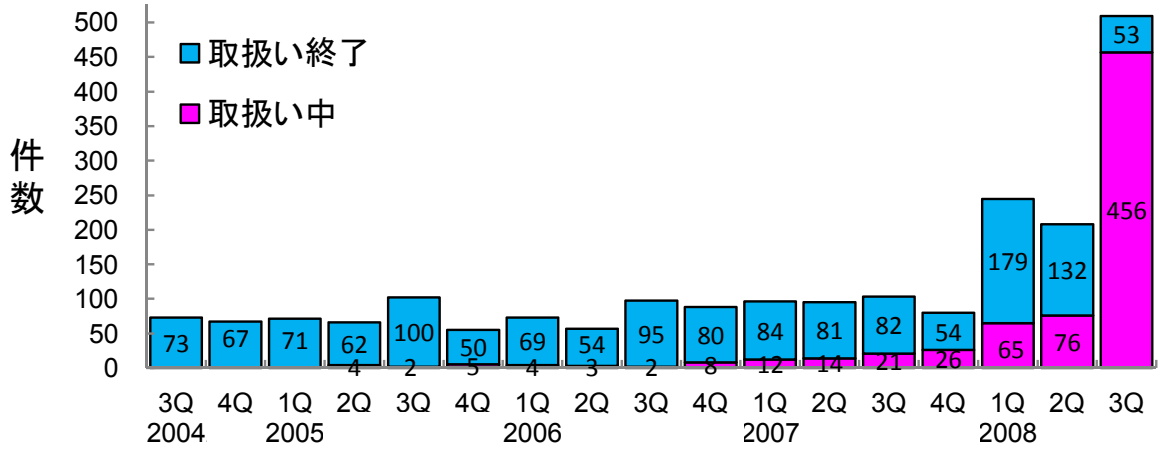


図3. ウェブサイトに関して各四半期に届出のあったものの現在の状況

[2] ソフトウェア製品開発者が修正完了したもの、脆弱性ではないと判断したもの、不受理のもの。
[3] ウェブサイト運営者が修正完了したもの、脆弱性ではないと判断したもの、連絡不可能なもの、不受理のもの。

2.ソフトウェア製品の脆弱性の処理状況

2008 年第 3 四半期のソフトウェア製品の脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN[4]で対策情報を公表したものは **25** 件でした。製品開発者からの届出のうち JVN で公表せず製品開発者が個別対応を行ったものは **0** 件、製品開発者が脆弱性ではないと判断したものは **0** 件、告示で定める届出の対象に該当せず不受理としたものは **12** 件でした。これらの取扱いを終了したものの合計は **37** 件（累計 **465** 件）です（表 2）。

表 2. ソフトウェア製品の脆弱性の終了件数

分類		件数	累計件数
修正完了	公表済み	**25** 件	**299** 件
	個別対応	**0** 件	**16** 件
脆弱性ではない		**0** 件	**34** 件
不受理		**12** 件	**116** 件
合計		**37** 件	**465** 件

この他、海外の CSIRT[5]から JPCERT/CC が連絡を受けた **18** 件（累計 **374** 件）を JVN で公表しました。これらの、公表済み件数の期別推移を図 4 に示します。

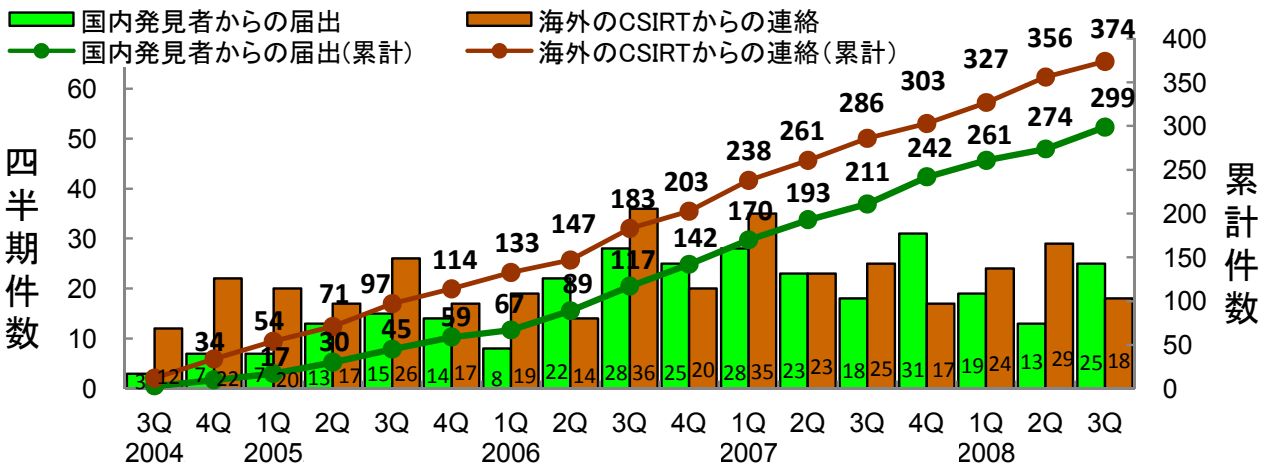


図4.ソフトウェア製品の脆弱性対策情報の公表件数

なお、2008 年第 3 四半期において、JVN で対策情報を公表した主なものは、以下のとおりです。

(1)「ウイルスセキュリティ」および「ウイルスセキュリティ ZERO」における脆弱性[6]

ソースネクスト株式会社が提供するウイルス対策ソフトの「ウイルスセキュリティ」および「ウイルスセキュリティ ZERO」のファイルのスキャン処理において圧縮ファイルの取扱いに問題があり、サービス運用妨害(DoS[7])状態となる脆弱性が存在しました。この弱点が悪用されると、「ウイルスセキュリティ」および「ウイルスセキュリティ ZERO」のスキャン処理が停止し、以降ウイルスが検知できなくなってしまうため、ウイルスに感染しやすくなる可能性があり、8 月 12 日に JVN で対策情報を公表しました。

---

[4] Japan Vulnerability Notes。脆弱性対策情報ポータルサイト。国内で利用されている製品の脆弱性対策情報を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。http://jvn.jp/

[5] Computer Security Incident Response Team。コンピュータセキュリティインシデント対応チーム。コンピュータセキュリティに関するインシデント（事故）への対応・調整・サポートをする組織です。

[6] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.3、別紙 P.5 表 1-2 項番 10 を参照下さい。

[7] Denial of Service。サービス不能状態。

(2) 複数のパナソニック コミュニケーションズ株式会社製ネットワークカメラにおけるクロスサイト・スクリプティングの脆弱性[8]

複数のパナソニック コミュニケーションズ株式会社製「ネットワークカメラ」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があり、7 月 31 日に JVN で対策情報を公表しました。

組込みソフトウェアの脆弱性は、この他に「複数のセンチュリー・システムズ株式会社製ルータにおけるクロスサイト・リクエスト・フォージェリの脆弱性」[9]、「iPod touch および iPhone に搭載されている Safari において証明書が不正に受け入れられる脆弱性」[10]の脆弱性対策情報を公表しました。

3.ウェブサイトの脆弱性の処理状況

2008 年第 3 四半期のウェブサイトの脆弱性の処理状況は、IPA が通知を行い、ウェブサイト運営者が修正を完了したものは **155** 件、ウェブサイト運営者が脆弱性ではないと判断したものは **5** 件、ウェブサイト運営者と連絡が不可能なものが **0** 件、告示で定める届出の対象に該当せず不受理としたものは **1** 件でした。これらの取扱いを終了したものの合計は **161** 件（累計 **1,386** 件）です（表 3）。

表 3. ウェブサイトの脆弱性の終了件数

分類	件数	累計件数
修正完了	**155** 件	**1133** 件
脆弱性ではない	**5** 件	**162** 件
連絡不可能	**0** 件	**7** 件
不受理	**1** 件	**84** 件
合計	**161** 件	**1,386** 件

これらのうち、修正完了件数の期別推移を図 5 に示します。

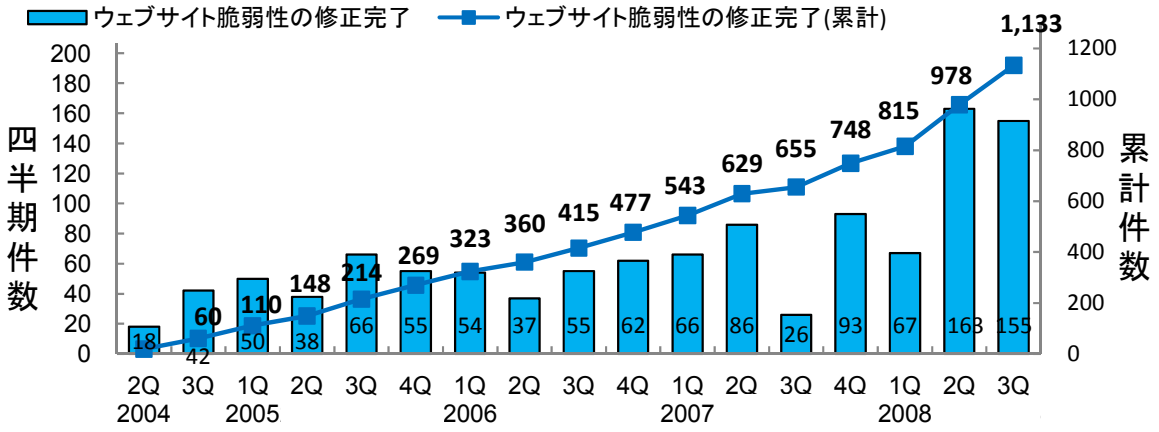


図5.ウェブサイトの脆弱性の修正完了件数

3.1 届出のあったウェブサイトの運営主体の内訳と脆弱性の種類

今四半期に脆弱性の届出のあった対象ウェブサイトの運営主体別内訳は、企業合計が 53%、政府機関が 6%、地方公共団体が 34%、団体（協会・社団法人）が 3%、個人が 3%などとなっています（図 6）。

また、今四半期に届出のあったウェブサイトの脆弱性の種類の内訳は、DNS(Domain Name System)[11]情報の設定不備が 56%、クロスサイト・スクリプティングが 18%、SQL インジェクションが 14%、ディレクトリ・トラバーサルが 7%、セッション管理の不備が 1%などとなっています（図 7）。

広く知れ渡っている脆弱性が数多く届出られており、ウェブサイト開発者は既知の脆弱性を認識し、ウェブサイトの企画・設計段階からのセキュリティの考慮が必要です。

---

[8] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.3、別紙 P.5 表 1-2 項番 9 を参照下さい。
[9] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0、別紙 P.4 表 1-2 項番 5 を参照下さい。
[10] 本脆弱性の深刻度=レベル I（注意）、CVSS 基本値=2.6、別紙 P.6 表 1-2 項番 21 を参照下さい。
[11] コンピュータがネットワークのどこに接続されているかを示す IP アドレスという数字の集まりを、www.ipa.go.jp のような人に覚えやすいドメイン表記と対応させるための情報を管理する仕組みです。

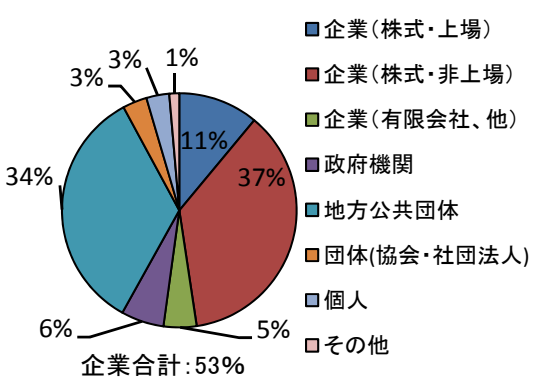


図6.ウェブサイトの運営主体（2008年第3四半期）

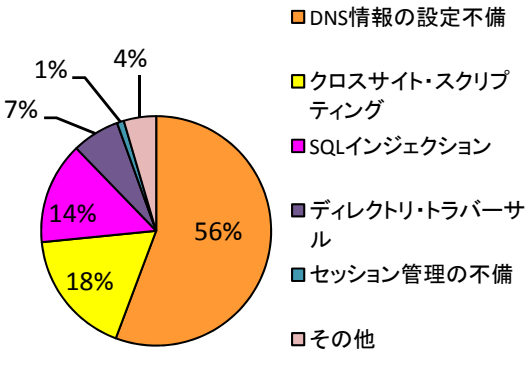


図7.ウェブサイトの脆弱性の種類（2008年第3四半期）

3.2 2008 年 8 月から DNS キャッシュポイズニングの脆弱性の届出が激増

図 7 に示すように、2008 年第 3 四半期は DNS 情報の設定不備の届出件数が突出して激増しました。これは、**DNS(Domain Name System)キャッシュポイズニングの脆弱性に関して、「実際に運用中のウェブサイトの DNS サーバに、対策を実施していないのではないか？」という旨の届出が激増**したためです。

図 8 に示すように 8 月 11 日の週から届出があり、9 月に入ってからは、毎週数十件にのぼっています（累計 283 件、9 月 30 日まで）。通常の脆弱性の届出は、毎週 10～20 件程度であることから、DNS キャッシュポイズニングの脆弱性の届出件数が突出して激増していると言えます。

この脆弱性に関しては、2008 年 7 月に複数の DNS サーバ製品の開発ベンダーから対策情報が公開され[12]、JPCERT/CC が 2008 年 7 月 9 日に注意喚起[13]を、また、IPA が 2008 年 7 月 24 日に緊急対策情報[14]を、2008 年 9 月 18 日に注意喚起[15]を発行しました。

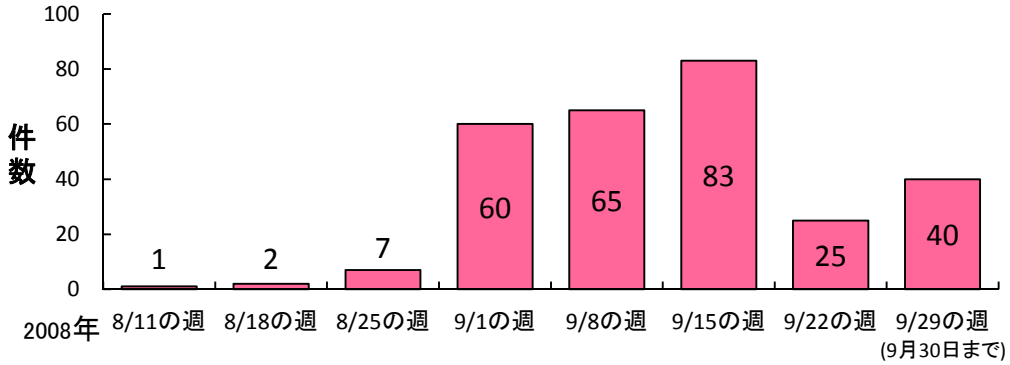


図8. DNSキャッシュポイズニングの脆弱性の届出件数の推移

3.3 DNS キャッシュポイズニングの脆弱性の脅威

DNS キャッシュポイズニングは、DNS キャッシュサーバ[16]に偽の情報(毒)を混入させる攻撃手法です。DNS キャッシュサーバは一般に、ネットワーク管理者がその組織内の構成員に提供するものです。このため、DNS キャッシュポイズニングの影響は、通常、当該組織内に限定されます。

---

[12] 脆弱性対策情報データベース JVN iPedia「複数の DNS 実装にキャッシュポイズニングの脆弱性」を参照。
http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html

[13] 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性。
http://www.jpcert.or.jp/at/2008/at080013.txt

[14] 複数の DNS 製品の脆弱性について。
http://www.ipa.go.jp/security/ciadr/vul/20080724-dns.html

[15] DNS キャッシュポイズニングの脆弱性に関する注意喚起。
http://www.ipa.go.jp/security/vuln/documents/2008/200809_DNS.html

[16] DNS サーバには、自分の管理しているドメインのみに関する情報を返す「DNS コンテンツサーバ」と、ユーザ等が利用するクライアントプログラムからの要求に応じて、ドメイン名から IP アドレスを、あるいは、IP アドレスからドメイン名を回答する「DNS キャッシュサーバ」があります。

また、一般的にウェブサイト運営者が外部の利用者へ提供するのは、DNS コンテンツサーバであり、DNS キャッシュサーバは提供しません。このため通常、ウェブサイトは DNS キャッシュポイズニングの影響を受けることはありません。

しかし、DNS キャッシュサーバが DNS コンテンツサーバを兼ねている構成のウェブサイトは少なくありません。このような構成で DNS の脆弱性の問題がある場合、ウェブサイト自体や第三者への脅威が発生する可能性があります。IPA はこれをウェブサイトの脆弱性として受け付けています。

脆弱性への対策を怠り悪用された場合、サイト運営組織内の利用者が、正しいウェブサイトの宛先を指定したにもかかわらず、知らぬ間に悪意のあるサイトに誘導され、金銭被害や個人情報漏えいの被害を受けてしまう可能性があります。結果として、サイト運営者は組織としての社会的な信頼の失墜や、経済的損失を被ることにもなりかねません。

脆弱性が届出られたウェブサイトの運営者は、政府機関、地方公共団体、民間企業など広範囲に渡っています。個人情報を扱っているような社会的影響の大きいウェブサイトの DNS サーバについても多数の届出があり、各サイトの運営者は早急な調査と対策実施が必要です。

3.4 ウェブサイトの脆弱性で 90 日以上対策が未完了のものは 179 件

IPA は、ウェブサイト運営者から脆弱性対策の返信がない場合、脆弱性が攻撃された場合の脅威を丁寧に解説するなど、1～2 カ月毎にメールや郵送手段などで脆弱性対策を促しています。また、今四半期は、特に修正が長期化しているウェブサイト運営者に面会するなど、更に脆弱性対策を促しました。

この結果、図 9 に示すように、ウェブサイトの脆弱性で 90 日以上も対策が完了していないものは、前四半期から **28** 件減少しました。しかし、今四半期で新たに **71** 件が 90 日以上となったため、**43** 件増加し累計で **179** 件（前四半期は **136** 件）となりました。また、300 日以上も対策が完了していないものが **10** 件増加し累計で **76** 件（前四半期は **66** 件）となりました。

ウェブサイトの情報が盗まれてしまう可能性のある SQL インジェクションのように、**深刻度の高い脆弱性でも修正が長期化しているものがあります。ウェブサイト運営者は脆弱性を攻撃された場合の脅威を認識し、早期に対策を講じる必要があります。**

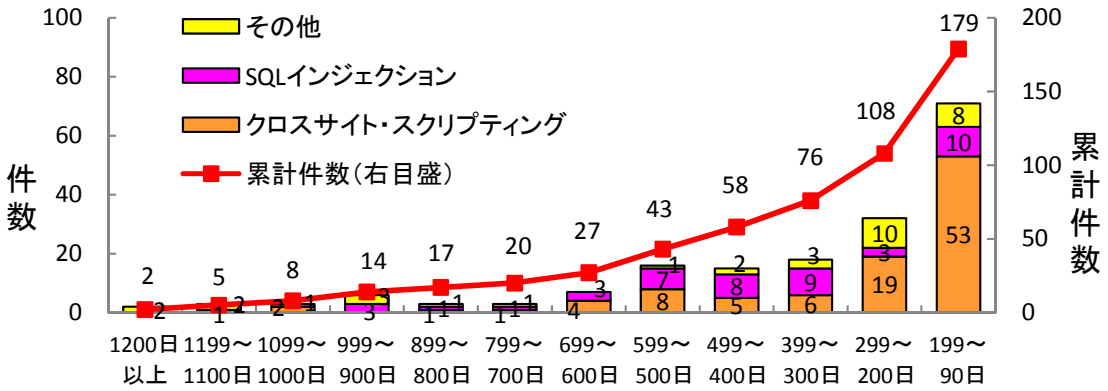


図9. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

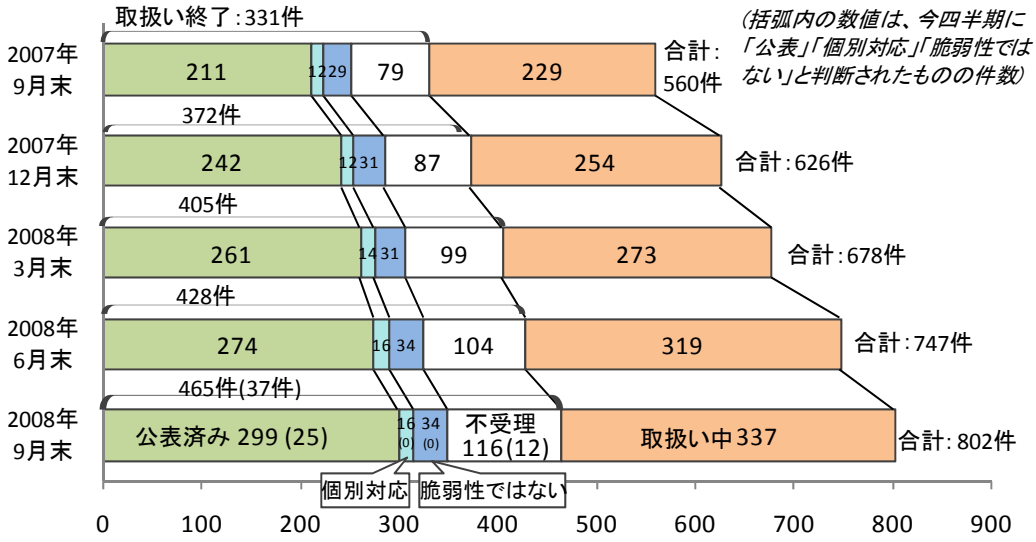
■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター 情報流通対策グループ 古田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: office@jpcert.or.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター 経営企画室 広報 江田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: pr@jpcert.or.jp

別紙

1. ソフトウェア製品の脆弱性の処理状況の詳細

1.1 ソフトウェア製品の脆弱性の処理状況

ソフトウェア製品の脆弱性関連情報の届出について、処理状況を図 1-1 に示します。今四半期に公表した脆弱性は、**25** 件（累計 **299** 件）です。また、「不受理」としたものは **12** 件（累計 **116** 件）です。



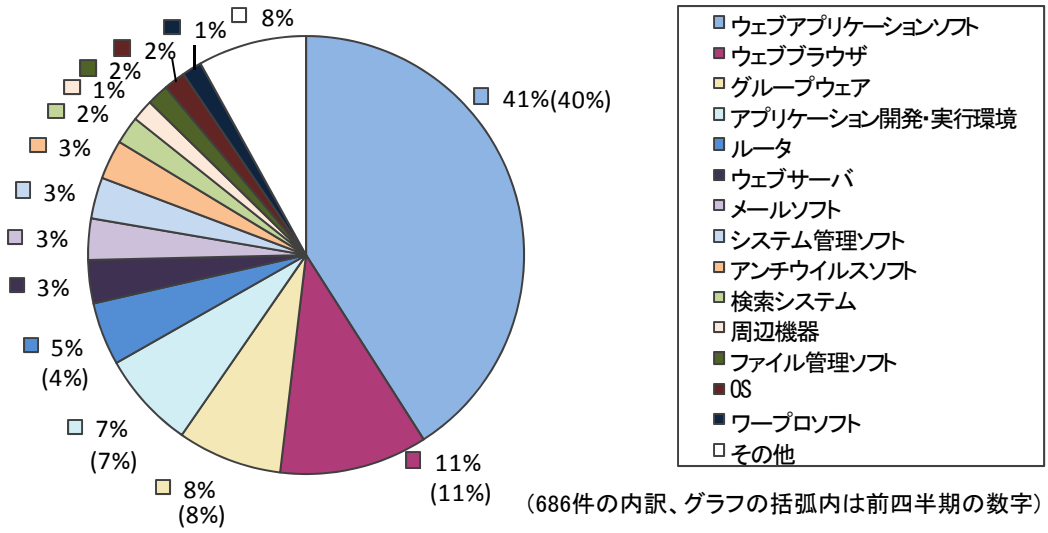
公表済み:	JVN で脆弱性への対応状況を公表したもの
個別対応:	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない:	製品開発者により脆弱性ではないと判断されたもの
不受理:	告示で定める届出の対象に該当しないもの
取扱い中:	製品開発者が調査、対応中のもの

図 1-1.ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

1.2 届出られた製品の種類

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 **802** 件のうち、不受理のものを除いた **686** 件の製品種類別の内訳を図 1-2 に示します。

図 1-2 に示すように、IPA に届出があった脆弱性には、「ウェブアプリケーションソフト」に関するものが多くあります。



(686件の内訳、グラフの括弧内は前四半期の数字)

※その他には、携帯機器、情報家電、IP電話、データベース、プロキシなどがあります。

図1-2.ソフトウェア製品の脆弱性 製品種類別内訳（届出受付開始から2008年9月末まで）

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 **802** 件のうち、不受理のものを除いた **686** 件について、オープンソースソフトウェアとそれ以外のソフトウェアの脆弱性の届出件数の推移を図 1-3 に示します。2005 年第 3 四半期以降、オープンソースソフトウェアの届出が増加し、今四半期も **21** 件の届出がありました。

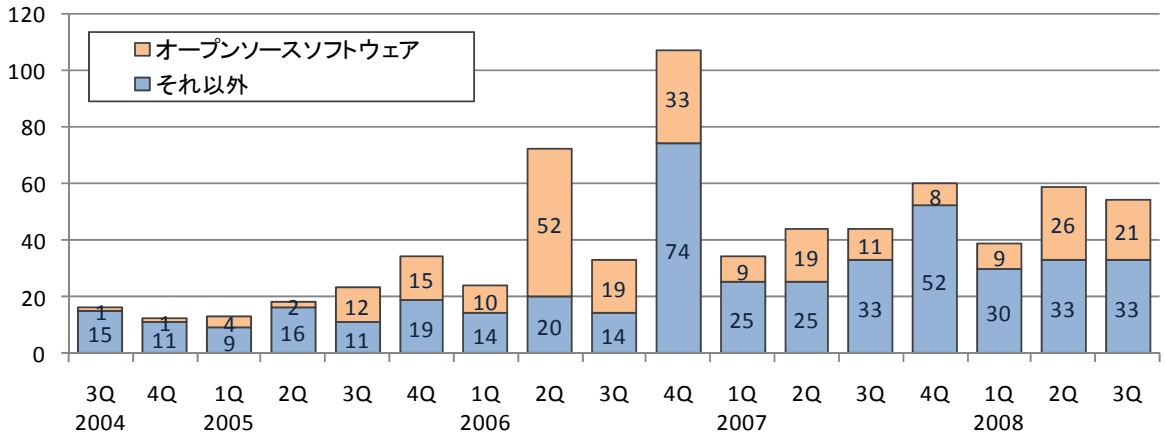
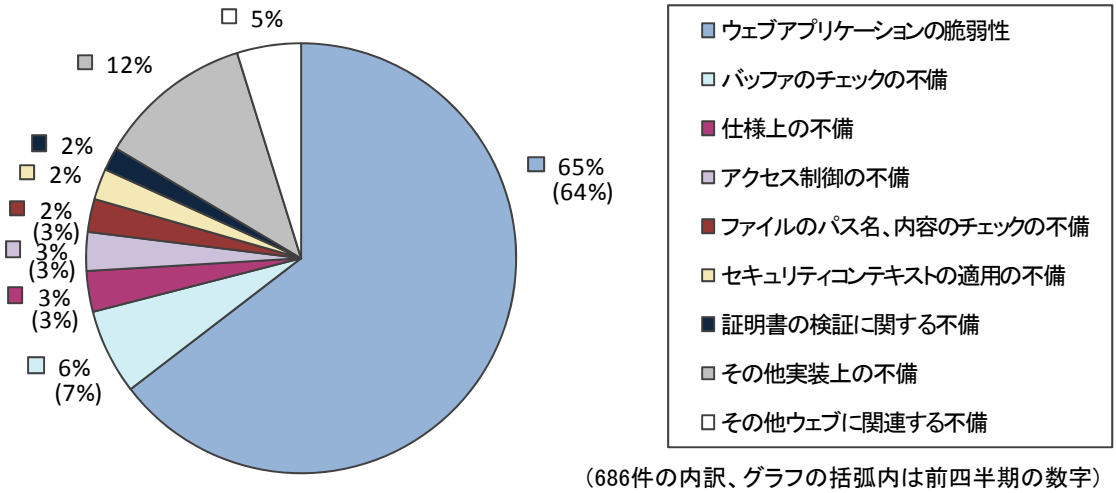


図1-3.オープンソースソフトウェアの脆弱性の届出件数　（686件の内訳）

1.3 脆弱性の原因と脅威

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 **802** 件のうち、不受理のものを除いた **686** 件の原因別の内訳を図 1-4 に、原因別の届出件数の推移を図 1-5 に、脅威別の内訳を図 1-6 に示します。

図 1-4 に示すように、脆弱性の原因は「ウェブアプリケーションの脆弱性」が最多であり、図 1-6 に示すように、脅威についても「任意のスクリプト実行」が最多となっています。これは、「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あり、そこに脆弱性が存在するためで、この傾向は図 1-5 に示すように、届出受付開始から続いています。



（686件の内訳、グラフの括弧内は前四半期の数字）

図1-4.ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2008年9月末まで）

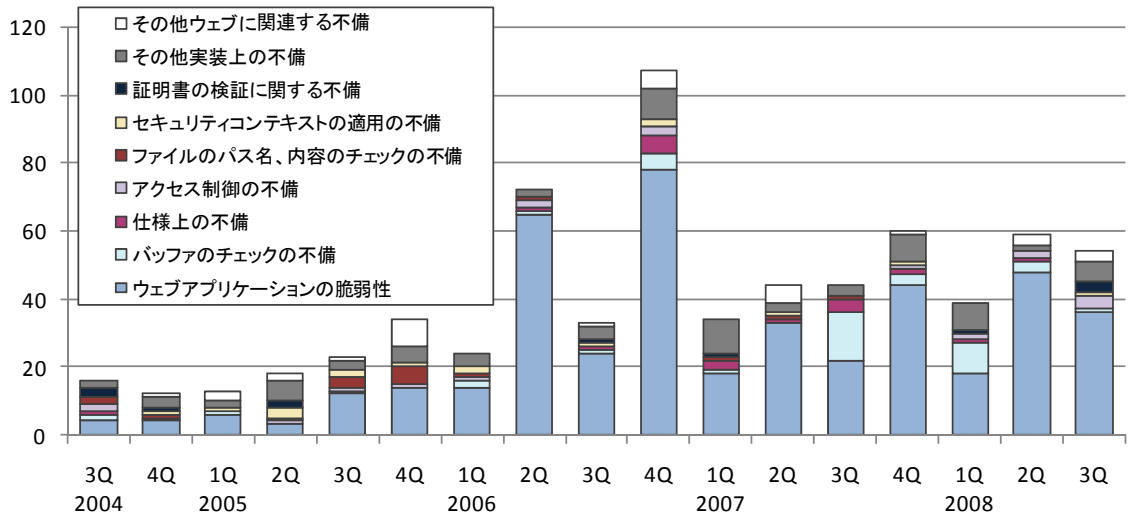
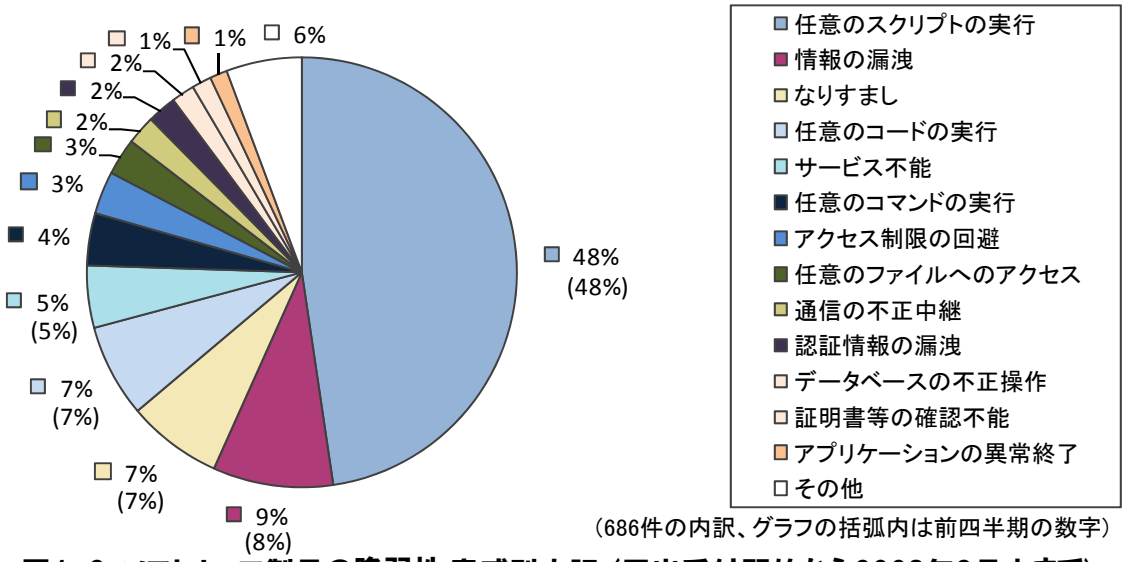


図1-5. ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2008年9月末まで）



（686件の内訳、グラフの括弧内は前四半期の数字）

図1-6. ソフトウェア製品の脆弱性 脅威別内訳（届出受付開始から2008年9月末まで）

1.4 ソフトウェア製品の脆弱性情報の調整および公表状況

JPCERT/CC は、表 1-1 に示す 2 種類の脆弱性関連情報について、日本国内の製品開発者等の関係者との調整、および海外 CSIRT[17] の協力のもと、海外の製品開発者との調整を行っています。これらの脆弱性関連情報に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）において公表しています（URL： http://jvn.jp/ ）

表 1-1. 脆弱性関連情報の提供元別 脆弱性公表件数

	情報提供元	今期	累計
①	国内の発見者から IPA に届出があったもの、および、製品開発者自身から自社製品の脆弱性、対策方法について連絡を受けたもの	25 件	299 件
②	海外 CSIRT 等と連携して公表したもの	18 件	374 件
	計	43 件	673 件

[17] CSIRT（Computer Security Incident Response Team）は、コンピュータセキュリティに関するインシデント（事故）への対応や調整、サポートをするチームのことです。

（1）国内の発見者および製品開発者から届出があり公表した脆弱性

届出受付開始から 2008 年 9 月末までの届出について、脆弱性関連情報の届出（表 1-1 の①）を受理してから製品開発者が対応状況を公表するまでに要した日数を図 1-7 に示します。届出受付開始から各四半期末までの 45 日以内に公表される件数が 32%であり、公表するまでに要した日数が増加する傾向にあります。製品開発者は脆弱性への早急な対応をお願いします。

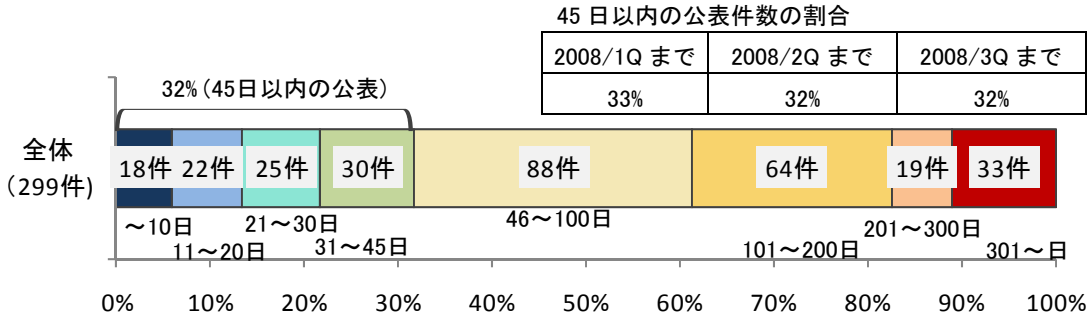


図1-7. ソフトウェア製品の脆弱性公表日数

表 1-2 に、国内の発見者、製品開発者から届出を受け、今四半期に公表した脆弱性を示します。オープンソースソフトウェアに関して開発者、開発コミュニティに通知し公表したものが 8 件（表 1-2 の*1）、複数の製品開発者のソフトウェア製品に影響がある脆弱性が 4 件（表 1-2 の*2）、組込みソフトウェア製品の脆弱性が 3 件（表 1-2 の*3）ありました。

表 1-2.2008 年第 3 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
1 (*1)	「FreeStyleWiki」におけるクロスサイト・スクリプティングの脆弱性	Wiki 構築ソフト「FreeStyleWiki」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 3 日	4.3
2 (*1)	「Redmine」におけるクロスサイト・スクリプティングの脆弱性	プロジェクト管理ソフト「Redmine」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、ウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 7 日	4.0
3	「WebLogic Server」および「WebLogic Express」に付属するプラグインにおけるディレクトリ・トラバーサルの脆弱性	アプリケーションサーバ「WebLogic Server」および「WebLogic Express」に付属するプラグインには、ディレクトリ・トラバーサルの脆弱性がありました。このため、遠隔の第三者により WebLogic Server および WebLogic Express が設置されているサーバ内のファイルを認証なしで閲覧される可能性がありました。	2008 年 7 月 18 日	5.0
4	LunarNight Laboratory 製「WebProxy」におけるクロスサイト・スクリプティングの脆弱性	プロキシサーバ構築ソフト「WebProxy」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 18 日	4.3
5 (*3)	複数のセンチュリー・システムズ株式会社製ルータにおけるクロスサイト・リクエスト・フォージェリの脆弱性	センチュリー・システムズが提供する複数のルータ製品のウェブ設定画面には、クロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、ウェブ設定画面にログインした状態で悪意あるページを読み込んだ場合、パスワードなどの設定が変更される可能性がありました。	2008 年 7 月 23 日	4.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
6	K's CGI 製「アクセスログ解析(jcode.pl 版)」におけるクロスサイト・スクリプティングの脆弱性	ホームページアクセス状況解析ソフト「アクセスログ解析(jcode.pl 版)」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 23 日	5.0
7	K's CGI 製「アクセスログ解析(Jcode.pm 版)」におけるクロスサイト・スクリプティングの脆弱性	ホームページアクセス状況解析ソフト「アクセスログ解析(jcode.pm 版)」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 23 日	5.0
8 (*1)	「Geeklog Forum Plugin」におけるクロスサイト・スクリプティングの脆弱性	コンテンツ管理システムである Geeklog の掲示板プラグイン「Geeklog Forum Plugin」には、、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 25 日	4.3
9 (*3)	複数のパナソニック コミュニケーションズ株式会社製「ネットワークカメラ」におけるクロスサイト・スクリプティングの脆弱性	複数のパナソニック コミュニケーションズ株式会社製「ネットワークカメラ」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 7 月 31 日	4.3
10	「ウイルスセキュリティ」および「ウイルスセキュリティ ZERO」におけるサービス運用妨害 (DoS) の脆弱性	ウイルス対策ソフト「ウイルスセキュリティ」および「ウイルスセキュリティZERO」には、サービス運用妨害 (DoS) の脆弱性がありました。細工された圧縮ファイルをスキャンした場合、以降のファイルのスキャンが行われなくなる可能性がありました。	2008 年 8 月 12 日	4.3
11 (*2)	「LacoodaST」におけるセッション固定の脆弱性	グループウェア「LacoodaST」には、セッション ID を正しく処理できない問題がありました。このため、第三者になりすまされてしまう可能性がありました。	2008 年 8 月 21 日	5.8
12 (*1) (*2)	「La!cooda WIZ」および「LacoodaST」におけるクロスサイト・スクリプティングの脆弱性	グループウェア「La!cooda WIZ」および「LacoodaST」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、ウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 8 月 21 日	4.3
13 (*1) (*2)	「La!cooda WIZ」および「LacoodaST」において任意の PHP スクリプトの実行が可能な脆弱性	グループウェア「La!cooda WIZ」および「LacoodaST」には、任意の PHP スクリプトファイルのアップロードが可能な脆弱性がありました。このため当該製品が設置されたサーバで任意の PHP スクリプトを実行される可能性がありました。	2008 年 8 月 21 日	6.5
14	アクアガーデンソフト製「mysql-lists」におけるクロスサイト・スクリプティングの脆弱性	MySQL データ閲覧ソフト「mysql-lists」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 8 月 26 日	4.3
15	株式会社ディーアイシー製「shop_v50」および「shop_v52」におけるクロスサイト・スクリプティングの脆弱性	ショッピングカートソフト「shop_v50」および「shop_v52」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 3 日	4.3

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
16	ハイ ノルマ (High Norm) 製「Sound Master 2nd」におけるクロスサイト・スクリプティングの脆弱性	音楽データ配布ソフト「Sound Master 2nd」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 9 日	4.3
17 (*1)	「Movable Type」におけるクロスサイト・スクリプティングの脆弱性	ウェブログ作成管理システム「Movable Type」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 9 日	4.3
18	「簡単 WEB サーバー」におけるディレクトリ・トラバーサルの脆弱性	Windows 用ウェブサーバ「簡単 WEB サーバー」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、遠隔の第三者により簡単 WEB サーバーが設置されているサーバ内のファイルを閲覧される可能性がありました。	2008 年 9 月 17 日	5.0
19	「簡単 WEB サーバー」におけるクロスサイト・スクリプティングの脆弱性	Windows 用ウェブサーバ「簡単 WEB サーバー」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 17 日	4.3
20 (*1)	「phpMyAdmin」におけるクロスサイト・スクリプティングの脆弱性	MySQL 操作・管理ソフト「phpMyAdmin」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 26 日	4.3
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
21 (*3)	iPod touch および iPhone に搭載されている「Safari」において証明書が不正に受け入れられる脆弱性	iPod touch および iPhone に搭載されている「Safari」には、サーバ証明書が不正に受け入れられる脆弱性がありました。このため、SSL 通信の盗聴などが行なわれる可能性がありました。	2008 年 7 月 14 日	2.6
22 (*1) (*2)	「La!cooda WIZ」および「LacoodaST」におけるクロスサイト・リクエスト・フォージェリの脆弱性	グループウェア「La!cooda WIZ」および「LacoodaST」には、クロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、当該製品にログインした状態で悪意あるページを読み込んだ場合、パスワードなどの設定を変更される可能性がありました。	2008 年 8 月 21 日	2.6
23	「Blogn(ぶろぐん)」におけるクロスサイト・リクエスト・フォージェリの脆弱性	ブログ作成ソフト「Blogn(ぶろぐん)」には、クロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、当該製品にログインした状態で悪意あるページを読み込んだ場合、意図せず Blogn(ぶろぐん) のコンテンツが編集される可能性がありました。	2008 年 8 月 29 日	2.6
24	「Blogn(ぶろぐん)」におけるクロスサイト・スクリプティングの脆弱性	ブログ作成ソフト「Blogn(ぶろぐん)」には、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 8 月 29 日	2.6
25	複数の Tor World 製 CGI スクリプトにおいて任意のスクリプトが実行される脆弱性	掲示板などの複数の Tor World 製 CGI スクリプトには、ウェブページを出力する際のエスケープ処理に漏れがありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2008 年 9 月 10 日	2.6

(*1):オープンソースソフトウェア製品の脆弱性
(*2):複数開発者・製品に影響がある脆弱性
(*3):組込みソフトウェアの脆弱性

（2）海外 CSIRT 等と連携して公表した脆弱性

JPCERT/CC が海外 CSIRT 等と連携して公表した脆弱性 18 件には、通常の脆弱性情報 11 件（表 1-3）と、対応に緊急を要する Technical Cyber Security Alert（表 1-4）の 7 件とが含まれます。これらの情報は、通常関連する登録済み製品開発者へ通知したうえ、JVN に掲載しています。

表 1-3.米国 CERT/CC[18]等と連携した脆弱性関連情報および対応状況

項番	脆弱性	対応状況
1	複数の DNS 実装にキャッシュポイズニングの脆弱性	複数製品開発者へ通知
2	BlackBerry Attachment Service の PDF 生成機能に任意のコードが実行可能な脆弱性	注意喚起として掲載
3	NetApp Data ONTAP における複数の脆弱性	注意喚起として掲載
4	Realnetworks RealPlayer の rjbdll.dll にバッファオーバーフローの脆弱性	注意喚起として掲載
5	RealNetworks RealPlayer の Shockwave Flash (SWF) ファイルの処理にバッファオーバーフローの脆弱性	注意喚起として掲載
6	Oracle Weblogic Apache connector プラグインにバッファオーバーフローの脆弱性	注意喚起として掲載
7	Postfix における権限昇格の脆弱性	複数製品開発者へ通知
8	NetBSD の MLD query パケット処理にサービス運用妨害(DoS)の脆弱性	複数製品開発者へ通知
9	InstallShield および FLEXnet Connect の通信処理の問題によるスクリプト実行の脆弱性	複数製品開発者へ通知
10	InstallShield の ActiveX コントロール Update Service Agent にバッファオーバーフローの脆弱性	注意喚起として掲載
11	ABB PCU400 にバッファオーバーフローの脆弱性	注意喚起として掲載

表 1-4.米国 US-CERT[19]と連携した脆弱性関連情報および対応状況

項番	脆弱性
1	Microsoft Office Snapshot Viewer ActiveX コントロールに脆弱性
2	Microsoft 製品における複数の脆弱性に対するアップデート
3	複数の DNS 実装にキャッシュポイズニングの脆弱性
4	Java における複数の脆弱性に対するアップデート
5	Microsoft 製品における複数の脆弱性に対するアップデート
6	Microsoft 製品における複数の脆弱性に対するアップデート
7	Apple 製品における複数の脆弱性に対するアップデート

[18] CERT/Coordination Center。1988 年のウイルス感染事件を契機に米国カーネギーメロン大学に設置された CSIRT。

[19] United States Computer Emergency Readiness Team。米国の政府系 CSIRT。

2. ウェブサイトの脆弱性の処理状況の詳細

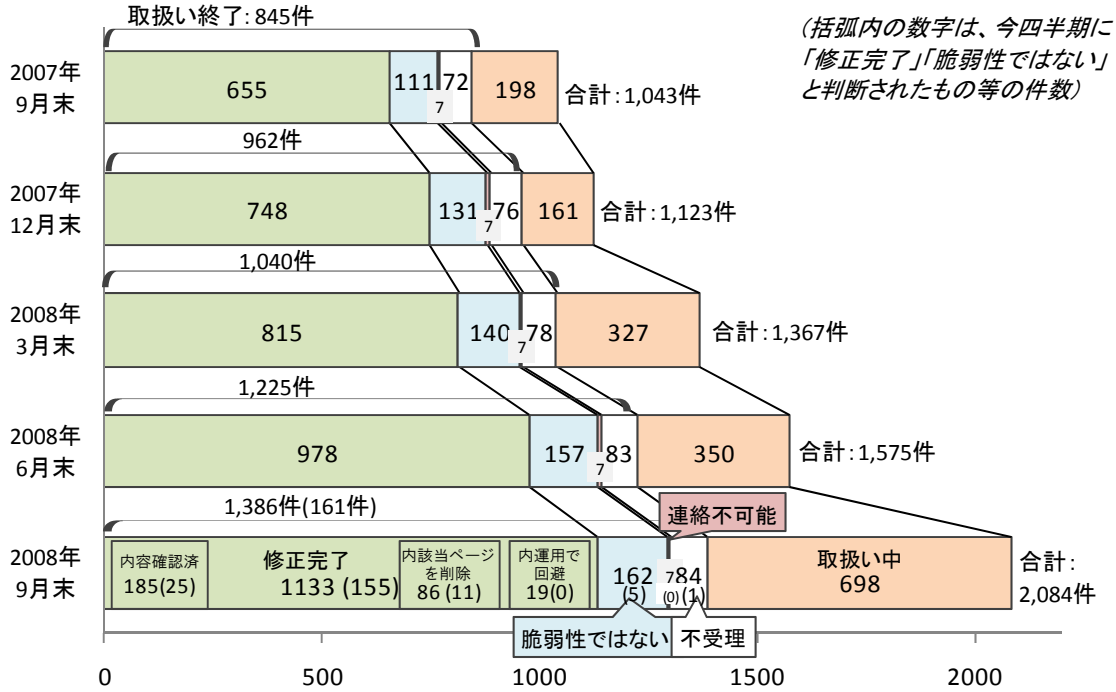
2.1 ウェブサイトの脆弱性の処理状況

ウェブサイトの脆弱性関連情報の届出について、処理状況を図 2-1 に示します。

図 2-1 に示すように、ウェブサイトの脆弱性について、今四半期中に処理を終了したものは **161** 件（累計 **1,386** 件）でした。このうち、「修正完了」したものは **155** 件（累計 **1133** 件）、ウェブサイト運営者により「脆弱性ではない」と判断されたものは **5** 件（累計 **162** 件）でした。なお、メールでウェブサイト運営者と連絡が取れない場合は、電話や郵送手段で連絡を試みたり、レンタルサーバ会社と連絡を試みたりしていますが、それでも、ウェブサイト運営者から回答がなく「取扱い不可能」なものは **0** 件(累計 **7** 件)です。「不受理」としたものは **1** 件（累計 **84** 件）でした。

取扱いを終了した累計 **1,368** 件のうち、「連絡不可能」「不受理」を除く累計 **1,277** 件（**93**%）は、指摘した点が解消されていることが、ウェブサイト運営者により報告されています。

「修正完了」したものうちのウェブサイト運営者からの依頼を受け、当該脆弱性が適切に修正されたかどうかを IPA が確認したものは **25** 件（累計 **185** 件）、ウェブサイト運営者が当該ページを削除することにより対応したものは **11** 件（累計 **86** 件）、ウェブサイト運営者が運用により被害を回避しているものは **0** 件（累計 **19** 件）でした。

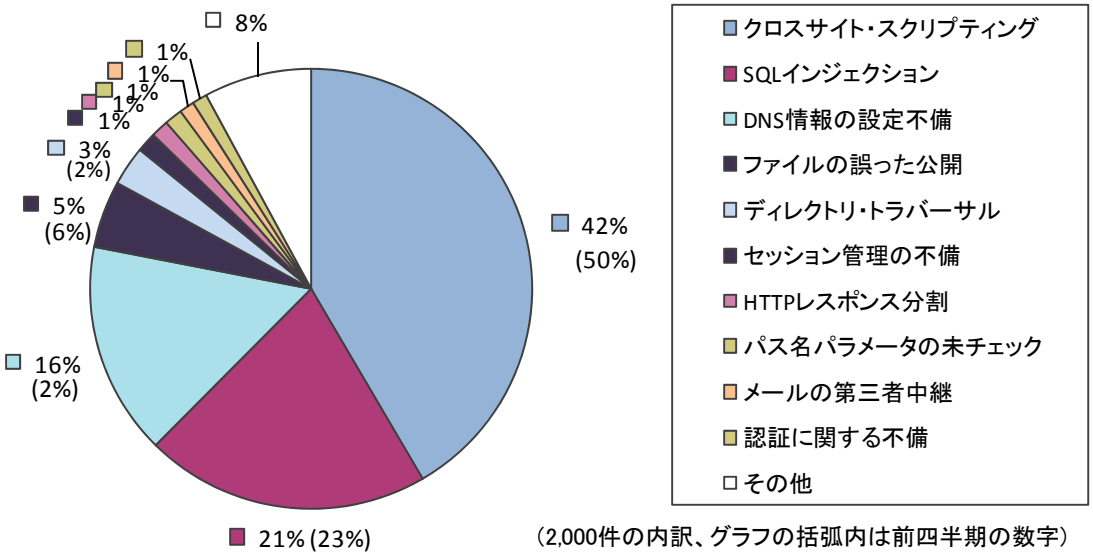


修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
確認済	：	修正完了のうち、IPA が修正を確認したもの
当該ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
運用で回避	：	修正完了のうち、運用により被害を回避しているもの
脆弱性ではない	：	ウェブサイト運営者により脆弱性はないと判断されたもの
連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
不受理	：	告示で定める届出の対象に該当しないもの
取扱い中	：	ウェブサイト運営者が調査、対応中のもの

図 2-1.ウェブサイト各時点における脆弱性関連情報の届出の処理状況

2.2 ウェブサイトの脆弱性の種類と脅威

届出受付開始から今四半期末までにIPAに届出られたウェブサイトの脆弱性関連情報**2,084**件のうち、不受理のものを除いた**2,000**件について、種類別内訳を図2-2に、種類別の届出件数の推移を図2-3に、脅威別内訳を図2-4に示します[20]。



（2,000件の内訳、グラフの括弧内は前四半期の数字）

図2-2.ウェブサイトの脆弱性 種類別内訳（届出受付開始から2008年9月末まで）

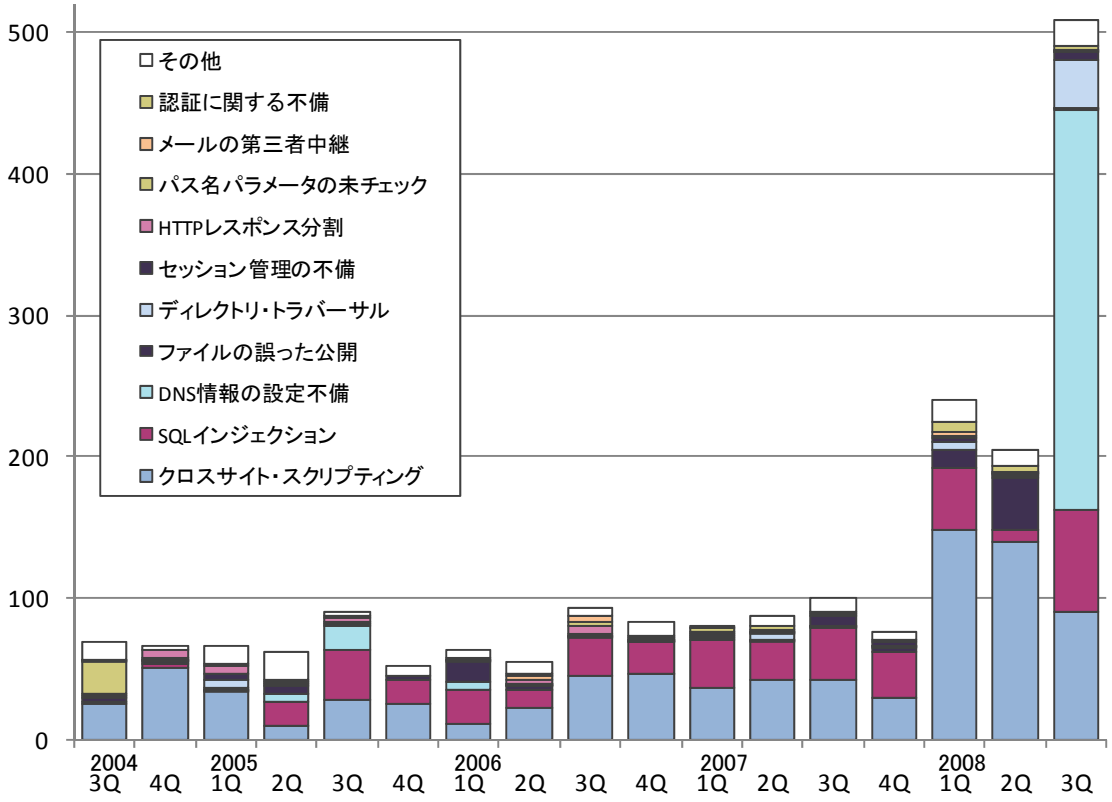
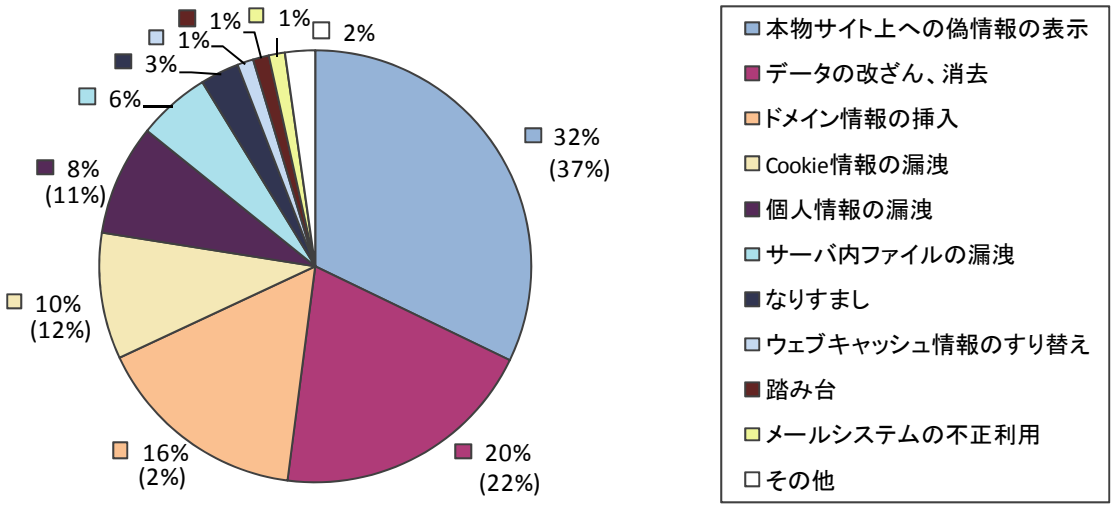


図2-3.ウェブサイトの脆弱性 種類別件数の推移（届出受付開始から2008年9月末まで）

[20] それぞれの脆弱性の詳しい説明については付表2を参照してください。



（2,000件の内訳、グラフの括弧内は前四半期の数字）

図2-4.ウェブサイトの脆弱性 脅威別内訳（届出受付開始から2008年9月末まで）

今四半期は「DNS 情報の設定不備」が多く届出られましたが（図 2-3）、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」が全体の 63%をしめます（図 2-2）。

また「クロスサイト・スクリプティング」や「SQL インジェクション」の脅威である、「本物サイト上への偽情報の表示」「データの改ざん、消去」「Cookie 情報の漏洩」が 62%をしめています（図 2-4）。

ウェブサイト運営者は、引き続き脆弱性を作りこまないように注意してください。

2.3 ウェブサイトの脆弱性の修正状況

届出受付開始から 2008 年 9 月末までの届出の中で、実際にウェブアプリケーションを修正したものについて、ウェブサイト運営者に脆弱性の詳細情報を通知してから修正されるまでに要した日数およびその傾向を、脆弱性の種類別に図 2-5 および図 2-6 に示します。全体の 56%の届出が 30 日以内、全体の 80%の届出が 90 日以内に修正されています。

90 日以内の修正件数の割合

2007/4Q まで	2008/1Q まで	2008/2Q まで	2008/3Q まで
78%	77%	81%	80%

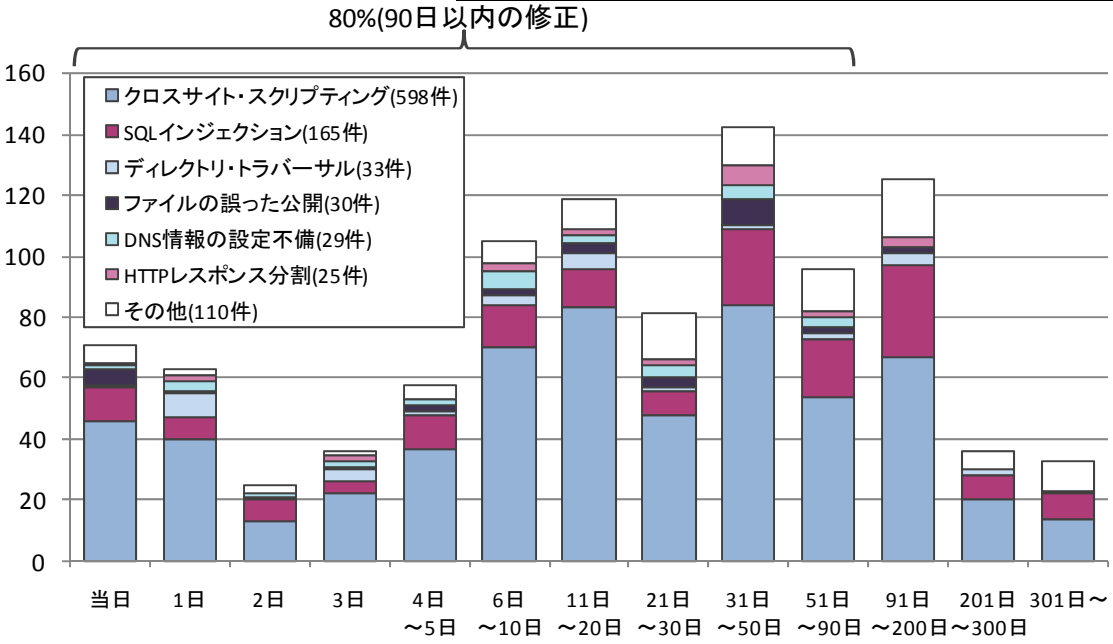


図2-5.ウェブサイトの修正に要した日数

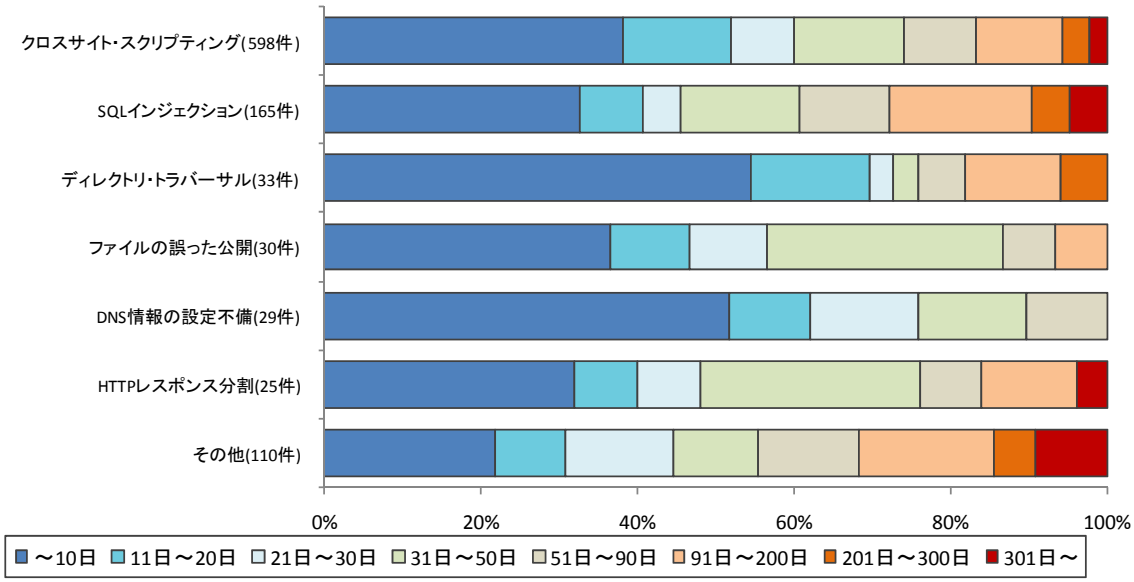


図2-6.ウェブサイトの修正に要した日数の傾向

3. 関係者への要望

脆弱性の修正を促進していくための、各関係者への要望は以下のとおりです。

(1)ウェブサイト運営者

多くのウェブサイトのソフトウェアに脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェアを利用しているかを把握し、脆弱性対策を実施することが必要です。

なお、脆弱性の理解にあたっては、以下のコンテンツが利用できます。

「知っていますか？脆弱性（ぜいじゃくせい）」:

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

「安全なウェブサイト運営入門」:

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

(2)製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報について、「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整を進められるよう、「製品開発者リスト」への登録を求めます（URL：http://www.jpcert.or.jp/vh/）。また、製品開発者自身で脆弱性を発見、修正された場合も、利用者への対策情報の周知のために JVN を活用できます。JPCERT/CC もしくは IPA への連絡を求めます。

(3)一般インターネットユーザ

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がけていただくことが必要です。脆弱性があるソフトウェアを使い続けることは避けなければなりません。

(4)発見者

脆弱性関連情報の適切な流通のため、届出られた脆弱性関連情報は、脆弱性が修正されるまでの期間は第三者に漏れぬよう、適切に管理されることを要望します。

付表 1. ソフトウェア製品 脆弱性の原因分類

	脆弱性の原因	説明	届出において想定された脅威
1	アクセス制御の不備	アクセス制御を行うべき個所において、アクセス制御が欠如している	設定情報の漏洩 通信の不正中継 なりすまし 任意のスクリプトの実行 認証情報の漏洩
2	ウェブアプリケーションの脆弱性	ウェブアプリケーションに対し、入力された情報の内容の解釈や認証情報の取扱い、出力時の処理に問題がある。「クロスサイト・スクリプティング」攻撃や「SQL インジェクション」攻撃などに利用されてしまう	アクセス制限の回避 価格等の改ざん サービス不能 資源の枯渇 重要情報の漏洩 情報の漏洩 セッション・ハイジャック 通信の不正中継 なりすまし 任意のコマンドの実行 任意のスクリプトの実行 任意のファイルへのアクセス 認証情報の漏洩
3	仕様上の不備	RFC 等の公開された規格に準拠して、設計、実装した結果、問題が生じるもの。プロトコル上の不備がある場合、ここに含まれる	サービス不能 資源の枯渇
4	証明書の検証に関する不備	ウェブブラウザやメールクライアントソフトに証明書を検証する機能が実装されていない、または、検証が正しく行われずに、偽の証明書を受けいれてしまう	証明書の確認不能 なりすまし
5	セキュリティコンテキストの適用の不備	本来、厳しい制限のあるセキュリティコンテキストで取り扱うべき処理を、緩い制限のセキュリティコンテキストで処理してしまう	アプリケーションの異常終了 情報の漏洩 任意のコードの実行 任意のスクリプトの実行
6	バッファのチェックの不備	想定外の長さの入力が行われた場合に、長さをチェックせずバッファに入力してしまう。「バッファオーバーフロー」攻撃に利用されてしまう。	サービス不能 任意のコードの実行 任意のコマンドの実行
7	ファイルのパス名、内容のチェックの不備	処理の際のパラメータとして指定されているディレクトリ名やファイル名、ファイルの内容をチェックしていない。任意のディレクトリのファイルを指定できてしまい、「ディレクトリ・トラバーサル」攻撃に利用されてしまう。また、破損したファイルや不正に書き換えられたファイルを処理した際に不具合が生じる	アプリケーションの異常終了 サービス不能 資源の枯渇 任意のファイルへのアクセス 認証情報の漏洩

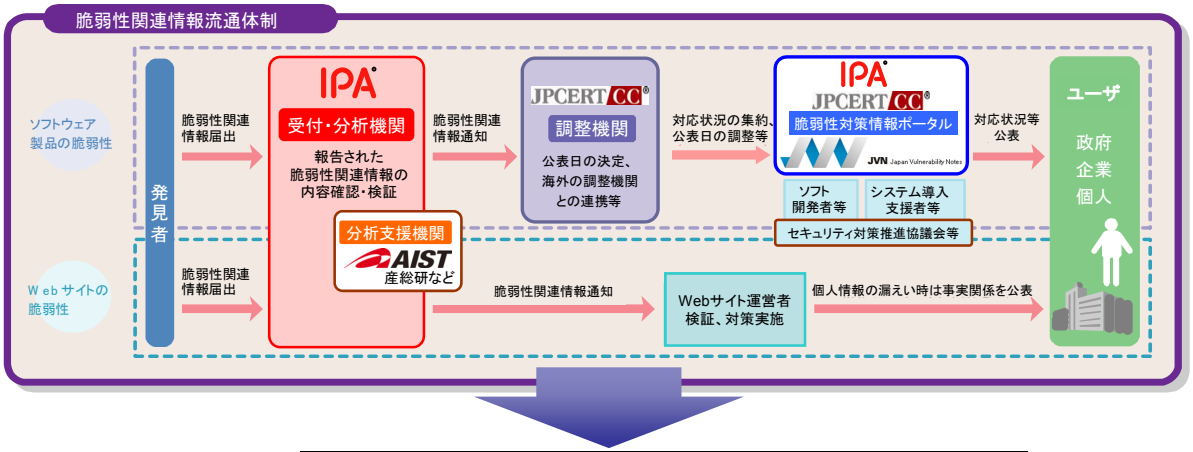
付表 2 ウェブサイト脆弱性の分類

	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
3	ディレクトリ･トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	個人情報の漏洩 サーバ内ファイルの漏洩
4	セッション管理の不備	高	セッション管理に、推測可能な情報を使用しているため、他のユーザの情報が容易に推測でき、他のユーザになりすまして、サービスを利用することができる	Cookie 情報の漏洩 個人情報の漏洩 なりすまし
5	SQL インジェクション	高	入力フォームなどへ SQL コマンド（データベースへの命令）を入力し、データベース内の情報の閲覧、更新、削除などができる	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去
6	DNS 情報の設定不備	高	DNS サーバに不適切な情報が登録されているため、第三者がそのドメイン名の持ち主であるかのようにふるまえてしまう	ドメイン情報の挿入
7	オープンプロキシ	中	外部の第三者により、他のサーバへのアクセスを中継するサーバとして利用され、不正アクセスなどの際にアクセス元を隠すための踏み台にされてしまう	踏み台
8	クロスサイト･スクリプティング	中	ユーザの Cookie 情報を知らないうちに転送させたり、偽の情報を表示させたりするような罠のリンクをユーザにクリックさせ、個人情報等を盗むことができる	Cookie 情報の漏洩 サーバ内ファイルの漏洩 個人情報の漏洩 データの改ざん、消去 なりすまし 本物サイト上への偽情報の表示
9	クロスサイト・リクエスト・フォージェリ	中	ユーザを罠のページに誘導することで、そのユーザが登録済みのサイトにひそかにアクセスさせ、登録情報の変更や商品の購入をさせることができる	データの改ざん、消去
10	HTTP レスポンス分割	中	攻撃者がユーザに対し、悪意のある要求をウェブサーバに送信するように仕向けることで、ウェブサーバからの応答を分割させて応答内容をすり替え、ユーザに対して偽のページを表示させることができる	ウェブキャッシュ情報のすり替え
11	セキュリティ設定の不適切な変更	中	ユーザに対し、ソフトウェアをインストールさせたり、ブラウザのセキュリティレベルを下げるよう指示することでクライアント PC のセキュリティ設定を低下させる	利用者のセキュリティレベルの低下
12	リダイレクタの不適切な利用	中	ウェブサーバに設置したリダイレクタが悪意あるリンクへの踏み台にされたり、そのウェブサイト上で別のサイト上のページを表示させられてしまう	踏み台 本物サイト上への偽情報の表示

	脆弱性の種類	深刻度	説明	届出において想定された脅威
13	フィルタリングの回避	中	ウェブサイトのサービスやブラウザの機能として提供されているフィルタリング機能が回避される問題。これにより、本来制限されるはずのウェブページを閲覧してしまう	利用者のセキュリティレベルの低下 なりすまし
14	OS コマンド・インジェクション	中	攻撃者がウェブアプリケーションを介してウェブサーバの OS コマンドを実行できてしまい、サーバ内ファイルの閲覧やシステム操作、不正なプログラムの実行などを行われてしまう	任意のコマンドの実行
15	メールの第三者中継	低	利用者が入力した内容を管理者が指定したメールアドレスに送信する機能で、外部の利用者が宛先メールアドレスを自由に指定できてしまい、迷惑メール送信の踏み台に悪用される	メールシステムの不正利用
16	HTTPS の不適切な利用	低	HTTPS による暗号化をしているが、暗号の選択や設定が十分でなかったり、ウェブサイトでのユーザへの説明に間違いがある、または、ウェブサイトの設計上、ユーザから証明書が確認できない	なりすまし
17	価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で書き換えられる。書き換えによる被害は、ウェブサイト側に限定される	データの改ざん

・API : Application Program Interface
・CGI : Common Gateway Interface
・DNS : Domain Name System
・HTTP : Hypertext Transfer Protocol
・HTTPS : Hypertext Transfer Protocol Security
・ISAKMP : Internet Security Association Key Management Protocol
・MIME : Multipurpose Internet Mail Extension
・RFC : Request For Comments
・SQL : Structured Query Language
・SSI : Server Side Include
・SSL : Secure Socket Layer
・TCP : Transmission Control Protocol
・URI : Uniform Resource Identifier
・URL : Uniform Resource Locator

付図１.「情報セキュリティ早期警戒パートナーシップ」（脆弱性関連情報取扱いの枠組み）



【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

※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター、産総研：独立行政法人　産業技術総合研究所