プレスリリース
2007 年 10 月 22 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 [2007 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:藤原 武平太) 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、2007 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。

今四半期の呼びかけ:
「製品開発者・ｳｪﾌﾞｻｲﾄ運営者は、脆弱性を攻撃された場合の脅威を認識し、早期に対応して下さい！」
－「知っていますか？脆弱性 (ぜいじゃくせい)」[2]を参考に－
※JPCERT/CC が脆弱性情報を調整する製品開発者の登録者数が累計で 200 社を突破しました。
※ウェブサイトに関する届出が累計で 1,000 件を突破しました。

1. 2007 年第 3 四半期の届出状況

表 1 に示すように、2007 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 **49** 件、ウェブサイト (ウェブアプリケーション) に関するもの **103** 件、合計 **152** 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 **560** 件、ウェブサイトに関するもの **1,043** 件、合計 **1,603** 件で、ウェブサイトに関する届出が全体の 3 分の 2 を占めています。

表 1. 2007 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	49 件	560 件
ウェブサイト	103 件	1,043 件
計	152 件	1,603 件

(1)四半期毎の届出状況の推移

図1[3]に示すように、届出受付開始 (2004 年 7 月 8 日) から各四半期末時点までの就業日 1 日あたりの届出件数が、近年着実に増加してきています。**今四半期で就業日 1 日あたり 2.03 件となり、2 件を突破しました。また、今四半期はウェブサイトに関する届出が 103 件と過去最高を記録し、累計で 1,000 件を突破しました。** 脆弱性関連情報の届出制度が浸透してきているものと考えています。

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	2005/2Q	2005/3Q	2005/4Q	2006/1Q	2006/2Q	2006/3Q	2006/4Q	2007/1Q	2007/2Q	2007/3Q
1.45	1.43	1.58	1.59	1.61	1.70	1.75	1.92	1.95	1.98	2.03

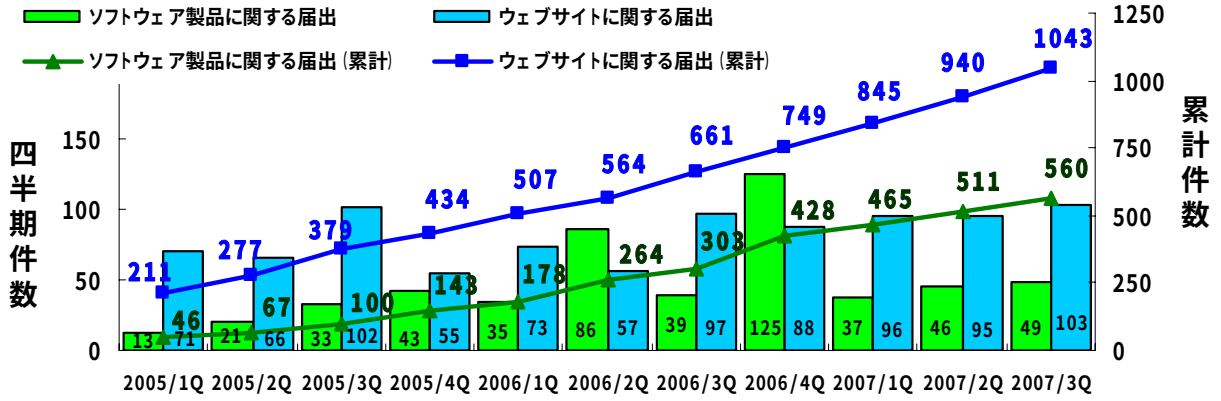


図1. 脆弱性関連情報の四半期別届出件数の推移

[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。

[2] 「知っていますか？脆弱性 (ぜいじゃくせい)」を 2007 年 7 月より公開しました。就業日 1 日当たり 1 千件を超えるアクセスがあり、好評に活用されています。http://www.ipa.go.jp/security/vuln/vuln_contents/

[3] 2007 年第 2 四半期に公表した四半期別届出件数の推移のグラフから、ソフトウェア製品に関する届出に関して、製品開発者が個別対応を行ったものを件数として追加するなどの変更をしました。

2.ソフトウェア製品の脆弱性の処理状況

表 2 に示すように、2007 年第 3 四半期にソフトウェア製品の脆弱性の修正が完了し JVN[4]で対策情報を公表したものは **18** 件（届出受付開始からの累計 **211** 件）、製品開発者からの届出のうち製品開発者が個別対応を行ったもの **2** 件（累計 **12** 件）、製品開発者が脆弱性ではないと判断したものは **0** 件（累計 **29** 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 **0** 件（累計 **74** 件）です。これらの取扱いを終了したものの合計は **20** 件（累計 **326** 件）です。詳細は別紙 1 の P.6 の 1 章を参照下さい。

表 2. ソフトウェア製品の脆弱性の処理件数

分類	件数	累計件数
公表済み	18 件	211 件
個別対応	2 件	12 件
脆弱性ではない	0 件	29 件
不受理	0 件	74 件
計	20 件	326 件

また、この他に、海外の CSIRT[5]から連絡を受けたもの **25** 件（累計 **286** 件）の脆弱性対策情報を JVN で公表しました。これらの、ソフトウェア製品の脆弱性対策情報の四半期別公表件数の推移は図 2 を参照下さい。

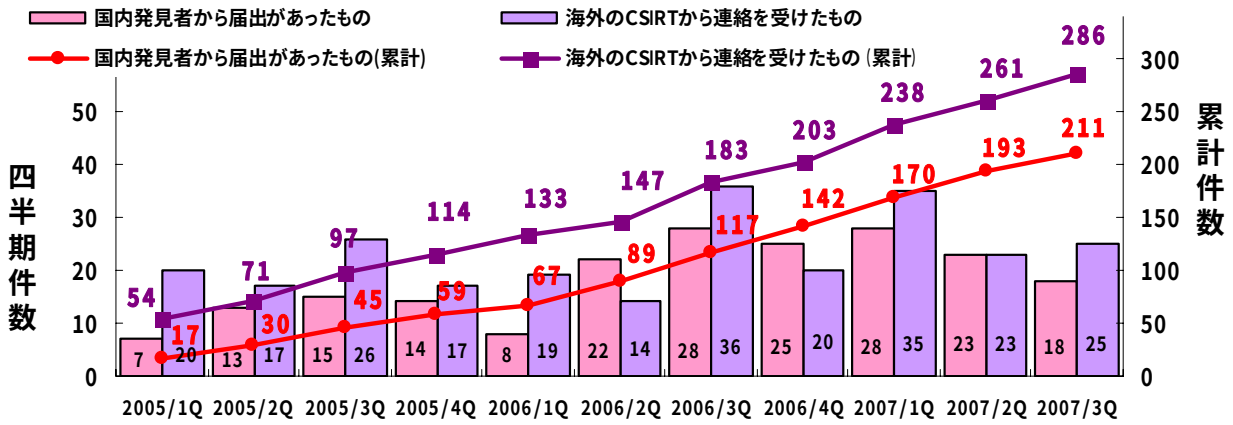


図2. ソフトウェア製品の脆弱性対策情報の四半期別公表件数の推移

(1)「Lhaplus」の脆弱性を注意喚起しました[6]

データ圧縮・解凍ソフトウェア「Lhaplus」に、バッファオーバーフローというセキュリティ上の弱点(脆弱性)が存在しました。「Lhaplus」は、lzh 形式のファイル圧縮形式に対応しているソフトウェアの一つとして、日本国内で広く利用されています。

脆弱性による影響が大きいことと、Lhaplus の普及状況より、この影響を受ける利用者が国内に広く存在すると判断し、9 月 21 日に注意喚起を行いました。

（詳細は 9 月 21 日付プレスリリースを参照。 http://www.ipa.go.jp/security/vuln/200709_Lhaplus.html
http://www.jpcert.or.jp/at/2007/at070020.txt ）

(2)「Flash Player」において任意の Referer ヘッダ[7]が送信可能な脆弱性の取扱いについて

ウェブ上で音声やアニメーションを再生するためのソフトウェア「Flash Player」には、任意の Referer ヘッダが送信可能な問題がありました。このため、Referer ヘッダを基にセキュリティ対策を行っているウェブアプリケーションは、そのセキュリティ対策が迂回されてしまう可能性がありました（別紙1の P.9 の表 1-2 項番 2）。

本件は、当初、Flash Player とは異なる国内製品（ウェブアプリケーション）の脆弱性として届出られたものでした。この問題の解決には、届出られた製品側で Referer ヘッダを基にしたセキュリティ対策を止めることや、

---

[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=6.8、別紙1の P.10 の表 1-2 項番 14 を参照下さい。

[7] HTTP のリクエストに含まれる情報で、リンク元を示す情報として送られる。通常、ウェブブラウザが自動的にリンク元のページの URL を Referer ヘッダとして、リンク先のサーバへ送っている。

ウェブブラウザ側で Referer ヘッダの送信方法を修正することも考えられました。しかし、本来、Referer ヘッダは、リンク元を示す情報としてクライアントからサーバへ架空の URL を送信してはならないとされています。

JPCERT/CC、IPA で調整を行った結果、米国 CERT/CC にも働きかけ、米国の Flash Player の開発者と交渉した結果、米国の Flash Player の開発者が修正を行い、7 月 11 日に脆弱性対策情報を公表しました。

(3)JPCERT/CC が脆弱性情報を調整する製品開発者の登録者数が累計で 200 社を突破しました

JPCERT/CC は、ソフトウェア製品の脆弱性が発生した際、影響を受ける可能性のある製品開発者を特定し、迅速かつ確実な情報を提供することを目的に、その連絡先となる製品開発者を製品開発者リストとして整備してきました。図 3 に示すように、この製品開発者リストに登録した製品開発者（製品脆弱性対策管理者）が 9 月末時点で 207 社となりました。**今後も脆弱性への早期対応を図るため、製品開発者リストへの登録を広く募集しています。**

(4)脆弱性対策情報データベース「JVN iPedia」[8]の登録件数が 4,000 件を突破しました

脆弱性対策情報データベース「JVN iPedia」は、約 3,600 件の登録情報で 4 月 25 日から提供開始しました。以来、図 4 に示すように、公開後も就業日 1 日当たり平均約 5 件の情報を登録し、9 月末時点で登録件数が 4,116 件となりました。**就業日 1 日当たり 2 千件を超えるアクセスがあり、好評に活用されています。**
（詳細は 9 月 14 日付プレスリリースを参照。 http://www.ipa.go.jp/security/vuln/200709_JVN_iPedia.html ）

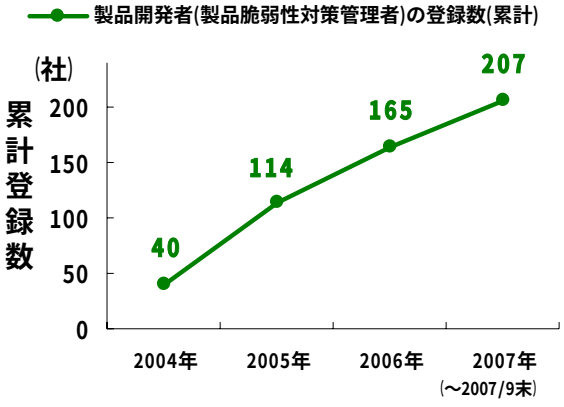


図3. 製品開発者リストへの登録数の推移

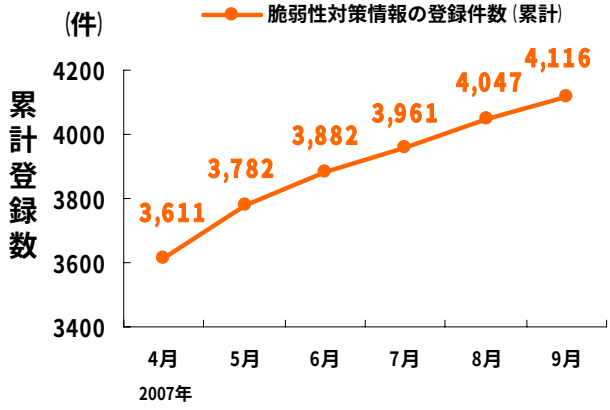


図4. JVN iPediaへの登録件数の推移

(5)脆弱性の深刻度評価を新バージョン CVSS v2[9]へ移行しました

ソフトウェア製品の脆弱性の深刻度評価に、FIRST[10]が推進している、共通脆弱性評価システム CVSS を採用しています。CVSS は、情報システムの脆弱性に対するオープンで汎用的な評価手法で、特定のベンダーに依存しない共通の評価方法として、脆弱性の深刻さを、製品利用者や SI 事業者、製品開発者などが、同一の基準の下で定量的に比較できるものです。現在、CVSS は 30 を超える組織で採用されています[11]。

スペインで開催された FIRST 年会議で CVSS の新バージョンである CVSS v2 が公表されたのを受け、脆弱性対策情報の公表ページ[12]、及び、JVN iPedia の深刻度評価を 8 月 20 日に CVSS v2 へ移行しました。

---

[8] 脆弱性対策情報データベース（ジェイブイエヌ アイ・ペディア）。脆弱性対策情報ポータルサイト「JVN」で公表した脆弱性対策情報約 400 件に加え、米国国立標準技術研究所 NIST が国立脆弱性データベース「NVD」で公開している約 2 万 5 千件の主に欧米英語圏の情報の中から、IPA が日本国内で使用されている製品に関連していると思われる情報を約 3,200 件を選び出し、その情報を翻訳し、公表を開始しました。http://jvndb.jvn.jp/

[9] Common Vulnerability Scoring System。http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

[10] Forum of Incident Response and Security Teams。コンピュータセキュリティインシデント対応チームフォーラム。CSIRT(Computer Security Incident Response Team)の国際的な連合体。http://www.first.org/

[11] CVSS の採用組織：http://www.first.org/cvss/eadopters.html

[12] http://www.ipa.go.jp/security/vuln/documents/index.html

JVN iPedia では脆弱性そのものの特性を評価した CVSS 基本値を公表しています。JVN iPedia の CVSS 計算ツール（図 5）を用い、製品利用者自身が脆弱性への対応を決めるための CVSS 現状値（攻撃コードの出現有無、対策情報の適用可否など）や CVSS 環境値（各組織での対象製品の利用範囲、攻撃を受けた場合の被害の大きさなど）を計算することが可能です。**就業日 1 日当たり 400 件を超えるアクセスがあり、好評に活用されています。今後も製品利用者は積極的に活用下さい。**

図5. JVN iPediaのCVSS計算ツール

3.ウェブサイトの脆弱性の処理状況

表 3 に示すように、2007 年第 3 四半期にウェブサイトの脆弱性の修正が完了したものは **26** 件（届出受付開始からの累計 **655** 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 **24** 件（累計 **111** 件）、ウェブサイト運営者と連絡が不可能なものが **0** 件（累計 **7** 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 **3** 件（累計 **72** 件）です。これらの取扱いを終了したものの合計は **53** 件（累計 **845** 件）です。詳細は別紙 1 の P.12 の 2 章を参照下さい。

表 3. ウェブサイトの脆弱性の処理件数

分類	件数	累計件数
修正完了	26 件	655 件
脆弱性ではない	24 件	111 件
連絡不可能	0 件	7 件
不受理	3 件	72 件
計	53 件	845 件

(1)ウェブサイトの脆弱性の届出が 1,000 件を突破しました

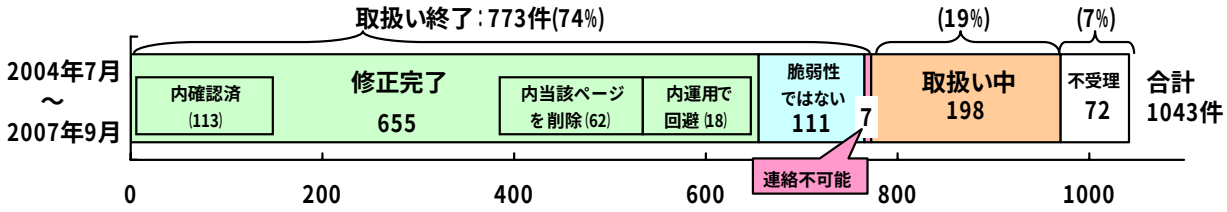
図 6 に届出受付開始（2004 年 7 月 8 日）から今四半期末までに届出られたウェブサイトの脆弱性の処理状況を示します。届出られた **1,043** 件のうち、「取扱い終了」は **773** 件（74%）、「取扱い中」は **198** 件（19%）、「不受理」は **72** 件（7%）となっており、**「取扱い中」を除く 845 件（81%）は取扱いの処理を終了しています。**

「取扱い終了」のうち、「修正完了」したものは **655** 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 **111** 件でした。なお、IPA はメールのほか、電話や郵送手段及びレンタルサーバ会社と通じてなどにより、ウェブサイト運営者への連絡を試みていますが、それでも、ウェブサイト運営者から回答がなく「連絡不可能」なものは **7** 件ありました。

「修正完了」のうち、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 が無償で確認したものは **113** 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 **62** 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 **18** 件でした。

「修正完了」した 655 件のうち 79%が、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 90 日以内に脆弱性の修正を完了しています（詳細は別紙 1 の P.14 の図 2-5 を参照下さい）。ウェブサイト運営者は脆弱性への素早い対応が必要です。



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
　内確認済　：　修正完了のうち、IPAが修正を確認したもの
　内当該ページを削除：　修正完了のうち、当該ページを削除して対応したもの
　内運用で回避　：　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
取扱い中　：ウェブサイト運営者が調査、対応中のもの
不受理　：告示で定める届出の対象に該当しないもの

図6. ウェブサイトの脆弱性の処理状況

(2)ウェブサイトの脆弱性で 300 日以上も対策が完了していないものが 50 件に達しました

IPA は、ウェブサイト運営者へ脆弱性の詳細情報を送付してから脆弱性対策の返信がない場合、当初 1 カ月毎に数回、その後 2～3 カ月毎にウェブサイト運営者へ、メールや郵送手段などで脆弱性対策を促しています。それにもかかわらず、300 日以上も対策が完了していないものが、図 7 に示すように **50** 件に達しました。

フィッシング詐欺に悪用されてしまう可能性のあるクロスサイト・スクリプティングや、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、早期に問題を解決することが必要です。**

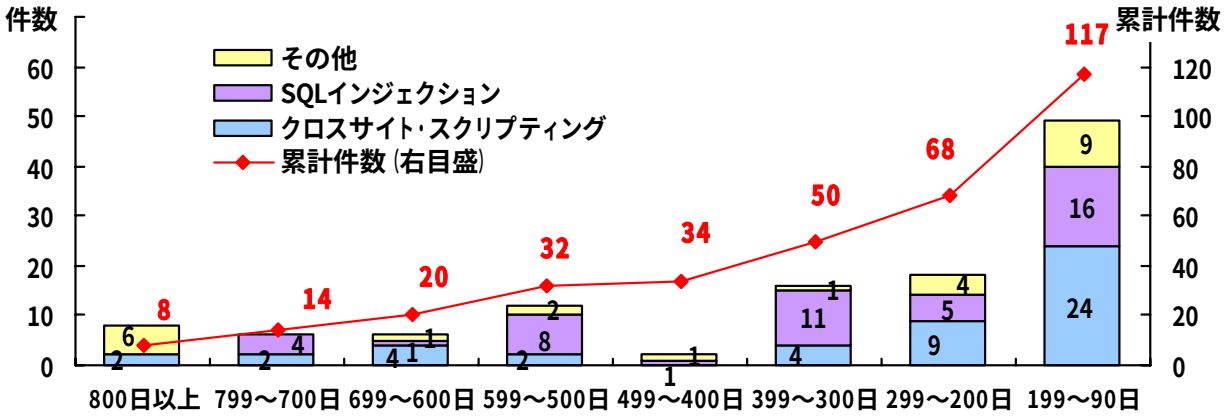


図7. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

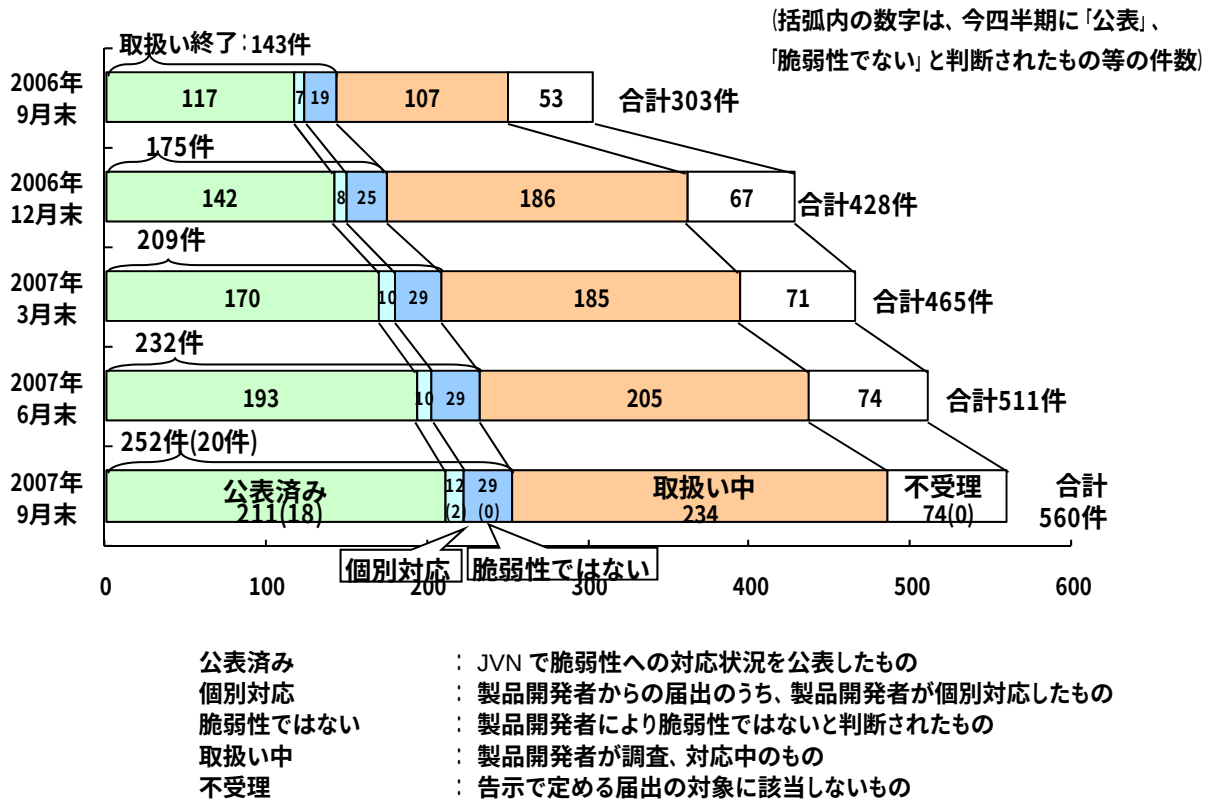
■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター
Tel: 03-3518-4600　Fax: 03-3518-4602　E-mail: office@jpcert.or.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503　Fax:03-5978-7510　E-mail: pr-inq@ipa.go.jp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

1. ソフトウェア製品の脆弱性関連情報の取扱いおよび調整

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、**18** 件（累計 **211** 件）でした。また、製品開発者が「個別対応」したものは **2** 件（累計 **12** 件）でした。



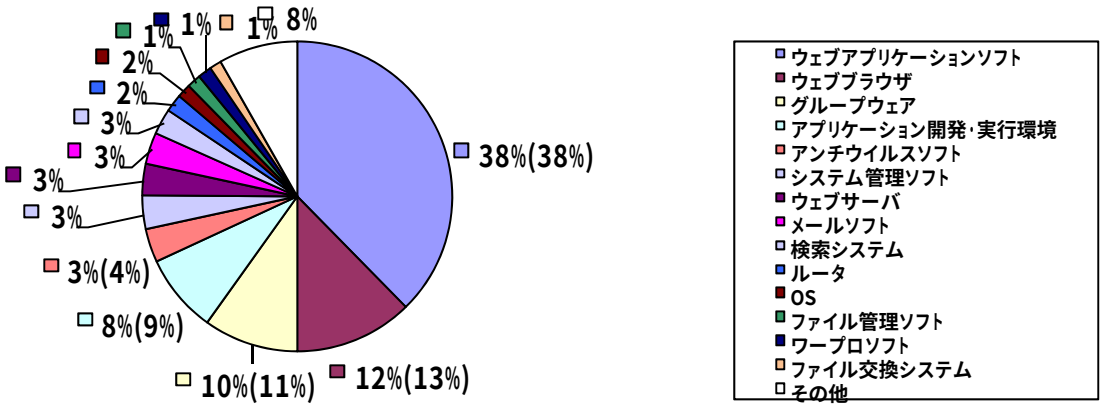
公表済み	：	JVN で脆弱性への対応状況を公表したもの
個別対応	：	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない	：	製品開発者により脆弱性ではないと判断されたもの
取扱い中	：	製品開発者が調査、対応中のもの
不受理	：	告示で定める届出の対象に該当しないもの

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 **560** 件のうち、不受理のものを除いた **486** 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。



（486 件の内訳、グラフの括弧内は前四半期の数字）

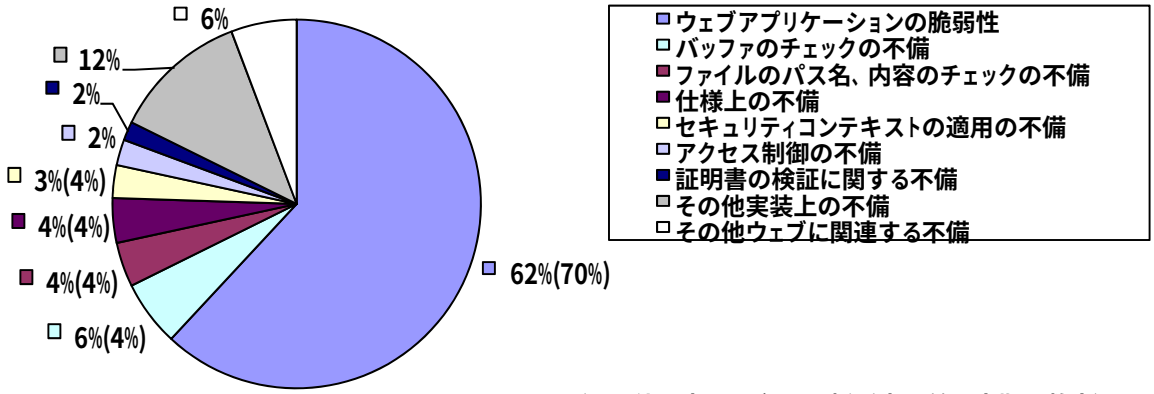
※　その他には、携帯機器、情報家電、パソコンの周辺機器、データベース、プロキシ等があります。

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 2007 年 9 月末まで）

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 **560** 件のうち、不受理のものを除いた **486** 件の原因別の内訳を図 1-3 に、原因別の届出件数の推移を図 1-4 に、脅威別の内訳を図 1-5 に示します。

図 1-3 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す。この傾向は図 1-4 に示すように 2 年以上も続いています。脅威については、図 1-5 に示すように、「任意のスクリプト実行」が最多となっています。



（486 件の内訳、グラフの括弧内は前四半期の数字）

図 1-3.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 2007 年 9 月末まで）[13]

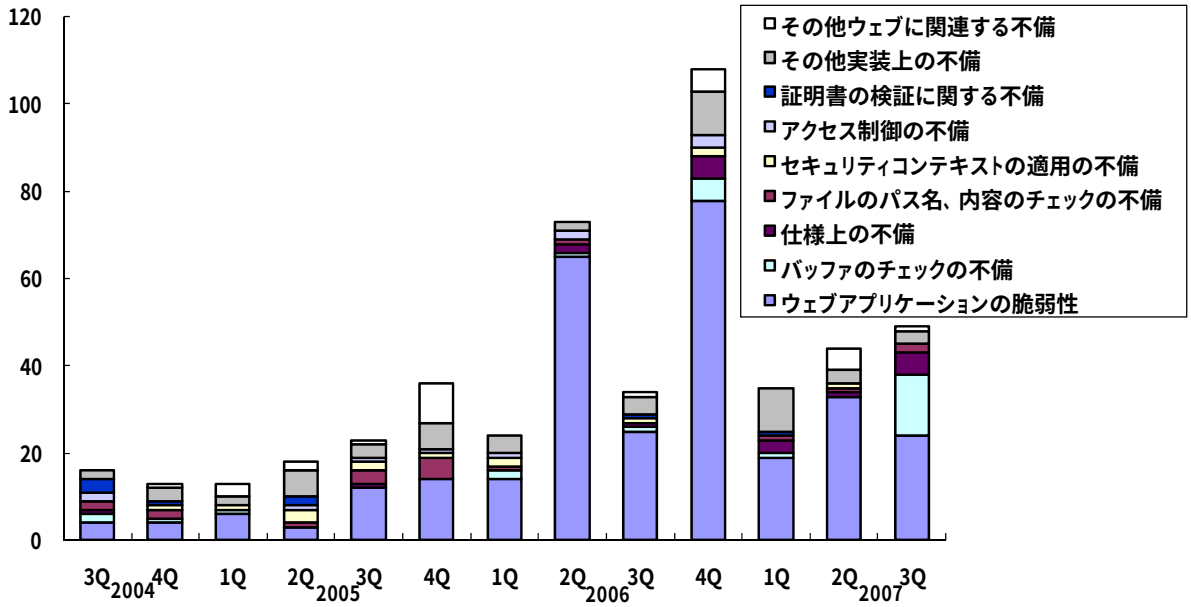
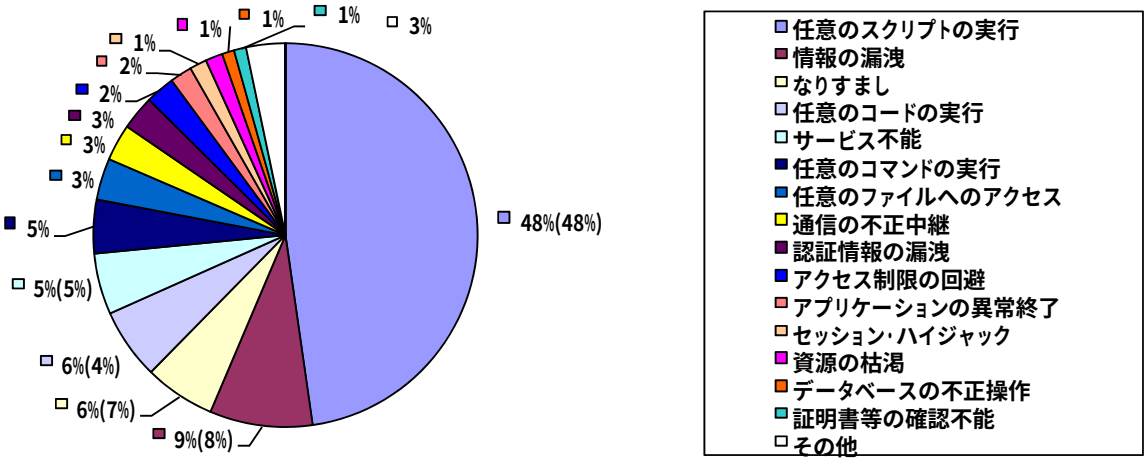


図 1-4.ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から 2007 年 9 月末まで）[14]

[13] それぞれの脆弱性の詳しい説明については付表 1 を参照してください。



(486 件の内訳、グラフの括弧内は前四半期の数字)

図 1-5.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 2007 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[14]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**	18	211
②	**海外 CSIRT 等と連携して公表したもの**	25	286
	計	43	497

(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 2007 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 1-6 に示します。45 **日以内に公表される件数が 36%と減少してきており、公表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が必要です。**

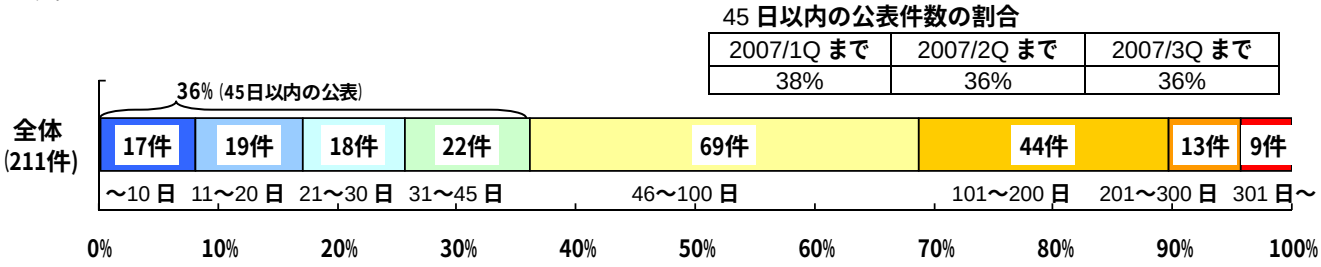


図 1-6.ソフトウェア製品の脆弱性 公表日数

[14] 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。

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 4 件（表 1-2 の*1）、製品開発者自身から自社製品に関する脆弱性対策情報について連絡を受け公表したものが 1 件（表 1-2 の*2）、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 1 件（表 1-2 の*3）、組込みソフトウェア製品の脆弱性が 1 件（表 1-2 の*4）ありました。

表 1-2. 2007 年第 2 四半期に JVN で公表した脆弱性

項番	脆弱性	未対策状態での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	KDDI 製ダウンロード CGI サンプルプログラムにおけるディレクトリ・トラバーサルの脆弱性	携帯端末向け CGI である KDDI 製「ダウンロード CGI サンプルプログラム」には、ディレクトリ・トラバーサルの問題があります。このため、第三者によりサーバ内の任意のファイルを閲覧される可能性があります。	2007 年 7 月 9 日	5.0
2	Flash Player において任意の Referer ヘッダが送信可能な脆弱性	ウェブ上で音声やアニメーションを再生するためのソフト「Flash Player」には、任意の Referer ヘッダが送信可能な問題があります。このため、Referer ヘッダを基にしたセキュリティ対策を迂回される可能性があります。	2007 年 7 月 11 日	4.3
3 (*1)	Nessus のレポート出力機能において任意のスクリプトが実行される脆弱性	コンピュータの脆弱性検査ソフト「Nessus」には、HTML ページを出力する際のエスケープ処理に漏れがあります。このため、第三者により意図しないスクリプトが実行されてしまう可能性があります。	2007 年 7 月 20 日	5.7
4 (*4)	Aruba Mobility Controller シリーズにおけるクロスサイト・スクリプティングの脆弱性	ウェブベースの管理画面を持つスイッチ製品「Aruba Mobility Controller」シリーズには、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す。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す。	2007 年 7 月 25 日	4.3
5	Safari における URL の表示偽装の脆弱性	Mac OS X に搭載されているウェブブラウザ「Safari」には、アドレスバーなどの URL 表示に問題があります。このため、第三者により偽装された URL に誘導され、フィッシング詐欺などの被害に遭う可能性があります。	2007 年 8 月 2 日	4.3
6	WebCart におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「WebCart」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す。このため、第三者により管理者用の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す。	2007 年 8 月 10 日	6.4
7 (*1)	Tuigwaa におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーション開発支援ソフト「Tuigwaa」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す。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す。	2007 年 8 月 27 日	4.3
8 (*1)	Mayaa におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーション開発支援ソフト「Mayaa」には、クロスサイト・スクリプティングの問題があります。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す。	2007 年 8 月 27 日	4.3
9	ショッピングバスケットプロにおけるディレクトリ・トラバーサルの脆弱性	ショッピングサイト構築ソフト「ショッピングバスケットプロ」には、ディレクトリ・トラバーサルの問題があります。このため、サーバ内の任意のファイル名やディレクトリ名を閲覧される可能性があります。	2007 年 8 月 31 日	5.0

項番	脆弱性	未対策状態での セキュリティ上の問題点	JVN 公表日	CVSS 基本値
10	futomi's CGI Cafe 製 全文検索 CGI におけるクロスサイト・スクリプティングの脆弱性	ウェブサイト用検索ソフト「futomi's CGI Cafe 製 全文検索 CGI」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す。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す。	2007 年 9 月 3 日	4.3
11	7-ZIP32.DLL におけるバッファオーバーフローの脆弱性	ファイル圧縮・展開用ライブラリ「7-ZIP32.DLL」には、バッファオーバーフローの脆弱性が存在します。このため、利用者のコンピュータ上で任意のコードを実行される可能性があります。	2007 年 9 月 5 日	6.8
12	Fuktommy.com 製 HTML プリプロセッサ付属の httpd.pl におけるディレクトリ・トラバーサルの脆弱性	ウェブサーバである「Fuktommy.com 製 HTML プリプロセッサ 付属の httpd.pl」には、ディレクトリ・トラバーサルの問題があります。このため、第三者によりサーバ内の任意のファイルを閲覧される可能性があります。	2007 年 9 月 6 日	5.0
13	Fuktommy.com 製 HTML プリプロセッサ付属の httpd.pl における任意の CGI ソースコードが閲覧可能な脆弱性	ウェブサーバである「Fuktommy.com 製 HTML プリプロセッサ 付属の httpd.pl」には、HTTP リクエスト中のファイル名を正しく処理できない問題があります。このため、第三者によりサーバ内の任意の CGI ソースコードを閲覧される可能性があります。	2007 年 9 月 6 日	5.0
14	Lhaplus におけるバッファオーバーフローの脆弱性	ファイル圧縮・展開ソフト「Lhaplus」には、バッファオーバーフローの脆弱性が存在します。このため、利用者のコンピュータ上で任意のコードを実行される可能性があります。	2007 年 9 月 21 日	6.8
15	Aipo におけるセッション固定の脆弱性	グループウェア「Aipo」には、セッション ID の固定化攻撃が行われてしまう問題があります。このため、第三者にあらかじめ用意したセッション ID を何らかの方法で利用者に送り込まれ、利用者のログインのタイミングを狙って、その利用者になりすまされてしまう可能性があります。	2007 年 9 月 28 日	4.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
16	弥生会計における認証情報の扱いに関する脆弱性	会計業務支援ソフト「弥生会計」のクイックナビゲータ機能には、ユーザの認証情報を暗号化せずに送信する問題があります。このため、第三者に通信を盗聴された場合、ユーザの認証情報が悪用され、なりすましなどの不正アクセスが行なわれる可能性があります。	2007 年 8 月 15 日	2.6
17 (*1) (*3)	Apache Tomcat の Host Manager におけるクロスサイト・スクリプティングの脆弱性	「Apache Tomcat」の管理者向けインターフェースソフト「Host Manager」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す。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す。	2007 年 8 月 15 日	2.6
18 (*2)	ソニー製指紋認証機能つき「ポケットビット」付属ソフトウェアにおける脆弱性	ソニー製 USB メモリ「ポケットビット」のうち指紋認証機能つきの製品に付属するソフトには、特定のフォルダを不可視にする問題があります。このため、不可視化されたフォルダを、第三者により意図しない用途で利用される可能性があります。	2007 年 9 月 7 日	2.6

(*1)：オープンソースソフトウェア製品の脆弱性
(*2)：製品開発者自身から届出られた自社製品の脆弱性
(*3)：複数開発者・製品に影響がある脆弱性
(*4)：組込みソフトウェア製品の脆弱性

⑵ 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 25 件には、通常の脆弱性情報 17 件（表 1-3）と、対応に緊急を要する Technical Cyber Security Alert（表 1-4）の 8 件とが含まれます。これらの脆弱性情報は、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[15]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	Lhaca におけるバッファオーバーフローの脆弱性	注意喚起として掲載
2	BIND9 の乱数生成に脆弱性	複数製品開発者へ通知
3	Atheros 社のワイヤレスネットワークドライバにおけるマネージメントフレームの取り扱いに関する脆弱性	複数製品開発者へ通知
4	Sun Java Web Start 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	一太郎シリーズに任意のコードが実行される脆弱性	特定製品開発者へ通知
6	RSA key reconstruction vulnerability	複数製品開発者へ通知
7	JRE (Java Runtime Environment) のフォント解析コードに権限昇格の脆弱性	注意喚起として掲載
8	Lhaz に任意のコードが実行される脆弱性	特定製品開発者へ通知
9	Trend Micro ServerProtect におけるバッファオーバーフローの脆弱性	注意喚起として掲載
10	Yahoo! メッセンジャーの webcam stream の処理にヒープオーバーフローの脆弱性	特定製品開発者へ通知
11	BIND8 の乱数生成に脆弱性	複数製品開発者へ通知
12	MSN メッセンジャーおよび Windows Live メッセンジャーの webcam ストリームの処理にヒープオーバーフローの脆弱性	特定製品開発者へ通知
13	MIT Kerberos 5 kadmind にバッファオーバーフローの脆弱性	複数製品開発者へ通知
14	MIT Kerberos 5 kadmind に権限昇格の脆弱性	複数製品開発者へ通知
15	web サービスにおいて認証情報が暗号化されずに通信される問題	注意喚起として掲載
16	Apple QuickTime に任意のコマンドが実行される脆弱性	注意喚起として掲載
17	Microsoft MFC FindFile() 関数にヒープ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[16]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	Microsoft 製品における複数の脆弱性	緊急案件として掲載
2	Adobe Flash Player に複数の脆弱性	緊急案件として掲載
3	Apple QuickTime に複数の脆弱性	緊急案件として掲載
4	Mozilla 製品における複数の脆弱性	緊急案件として掲載
5	Oracle 製品に複数の脆弱性	緊急案件として掲載
6	Microsoft 製品における複数の脆弱性	緊急案件として掲載
7	Trend Micro ServerProtect に複数の脆弱性	緊急案件として掲載
8	Microsoft 製品における複数の脆弱性	緊急案件として掲載

[15] CERT/Coordination Center。1988 年のウィ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。
[16] United States Computer Emergency Readiness Team。米国の政府系 CSIRT。

2. ウェブサイトの脆弱性関連情報の取扱い

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、今四半期中に、ウェブサイトの脆弱性の処理が終了したものは **50** 件（累計 **773** 件）でした。このうち、「修正完了」したものは **26** 件（累計 **655** 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 **24** 件（累計 **111** 件）でした。なお、メールのほか、電話や郵送手段及びレンタルサーバ会社を通じてなどで、ウェブサイト運営者との連絡を試みながら、回答がなく「取扱い不可能」なものは **0** 件（累計 **7** 件）でした。

取扱いを終了した累計 **773** 件のうち、「連絡不可能」を除く累計 **766** 件（**99%**）は、指摘され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確認されています。

「修正完了」したもののうち、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 **2** 件（累計 **113** 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 **1** 件（累計 **62** 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 **18** 件）でした。

このほか、「不受理」としたものは **3** 件（累計 **72** 件）でした。

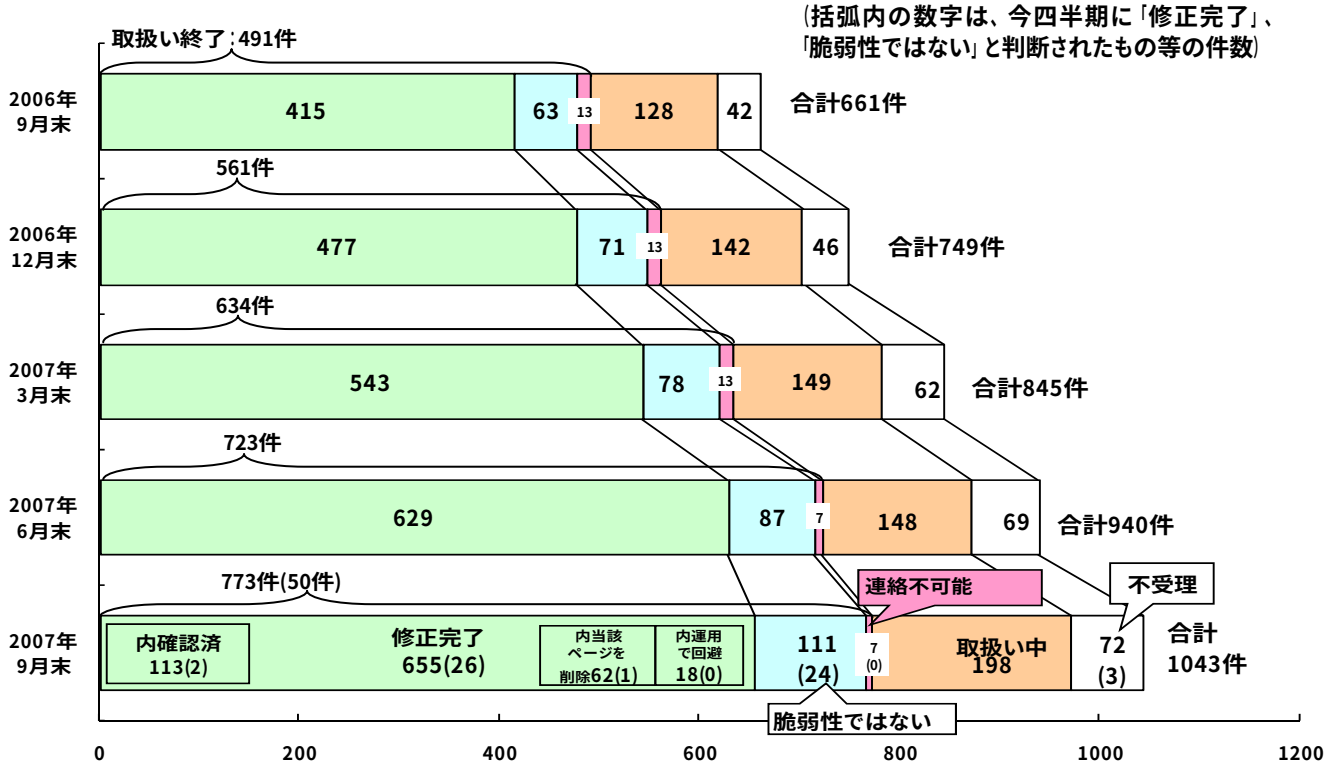


図 2-1. ウェブサイト各時点における脆弱性関連情報の届出の処理状況

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
取扱い中	：	ウェブサイト運営者が調査、対応中のもの
不受理	：	告示で定める届出の対象に該当しないもの

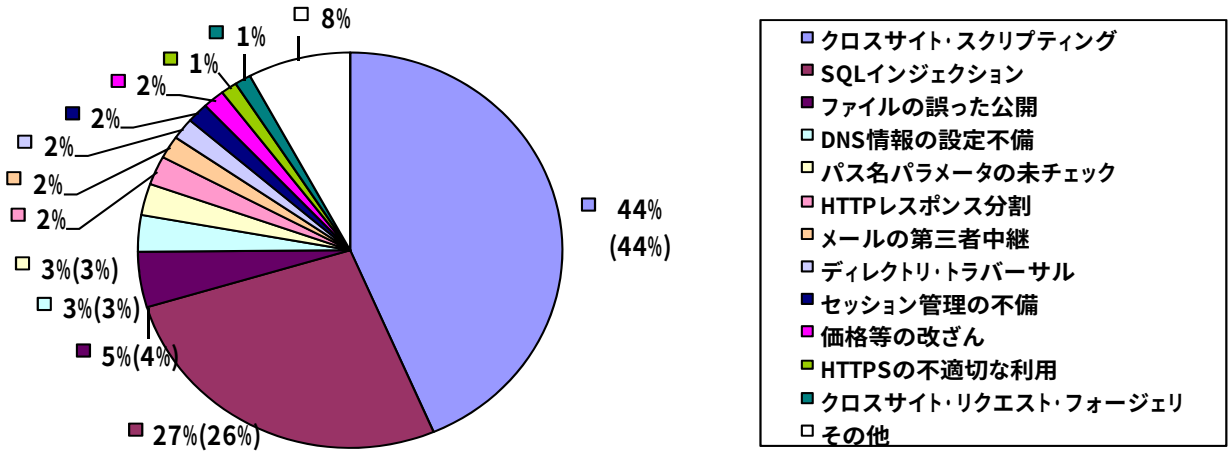
2.2 ウェブサイトの脆弱性の種類と脅威

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**1,043**件のうち、不受理のものを除いた**971**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。

今四半期も「クロスサイト・スクリプティング」が多く届出られ（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7割をしめます（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」「Cookie情報の漏洩」「データの改ざん、消去」が約7割をしめています（図2-4）。

ウェブサイト運営者は、脆弱性を作りこまないような注意が必要です。



（971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 2007 年 9 月末まで）[17]

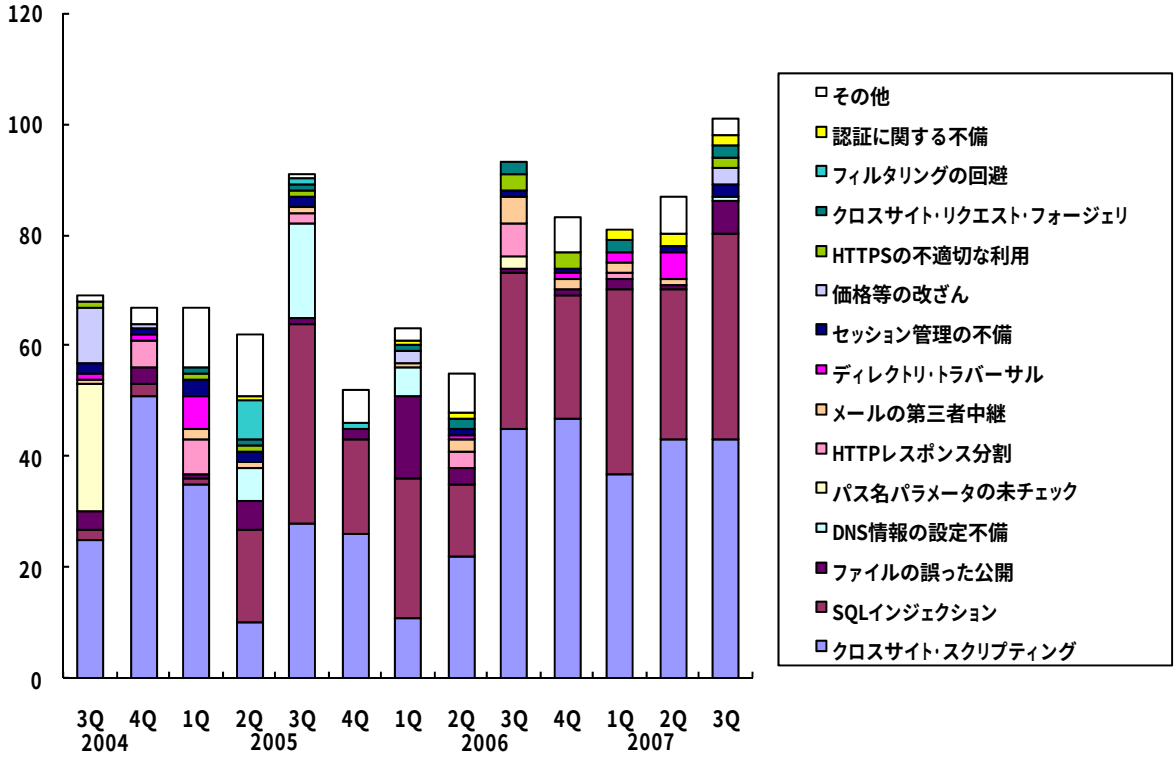
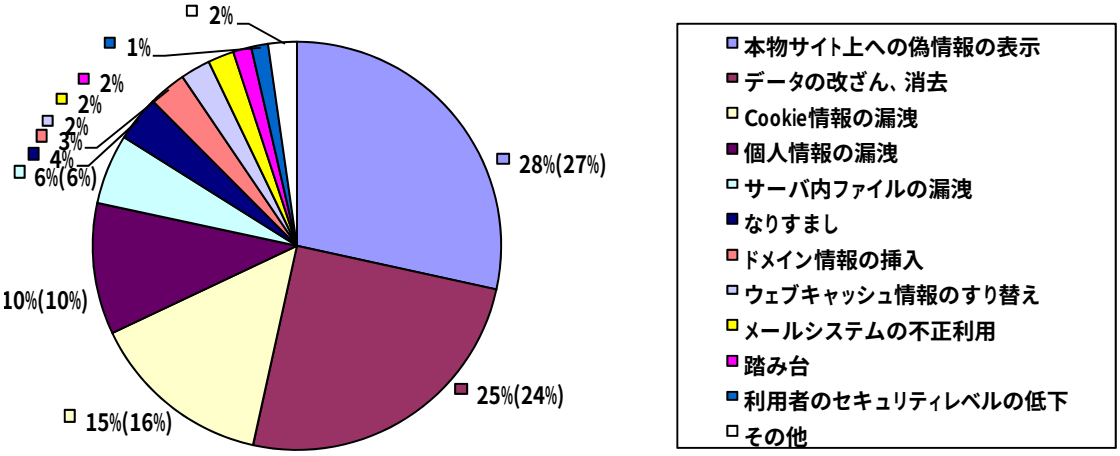


図 2-3. ウェブサイトの脆弱性種類別件数の推移（届出受付開始から 2007 年 9 月末まで）[18]

[17] 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。



(971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 2007 年 9 月末まで）

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 2007 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 54%の届出が 30 日以内、全体の 79%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

2007/1Q まで	2007/2Q まで	2007/3Q まで
81%	79%	79%

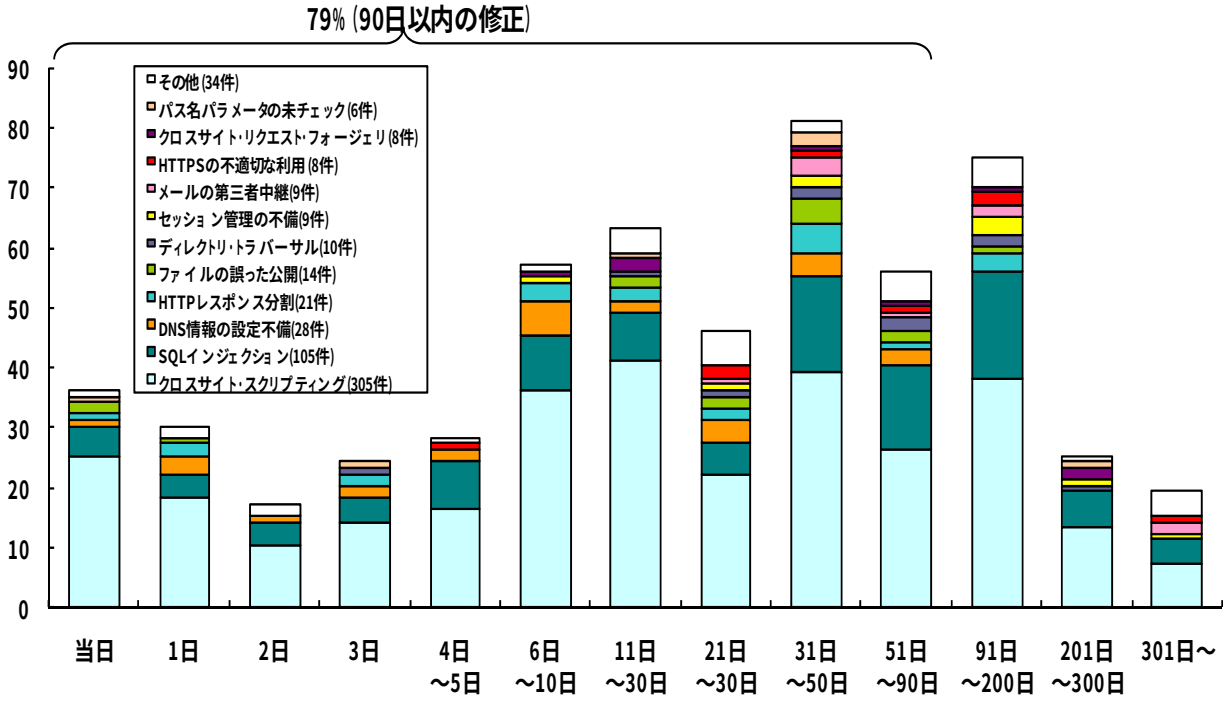


図 2-5.ウェブサイトの脆弱性修正に要した日数

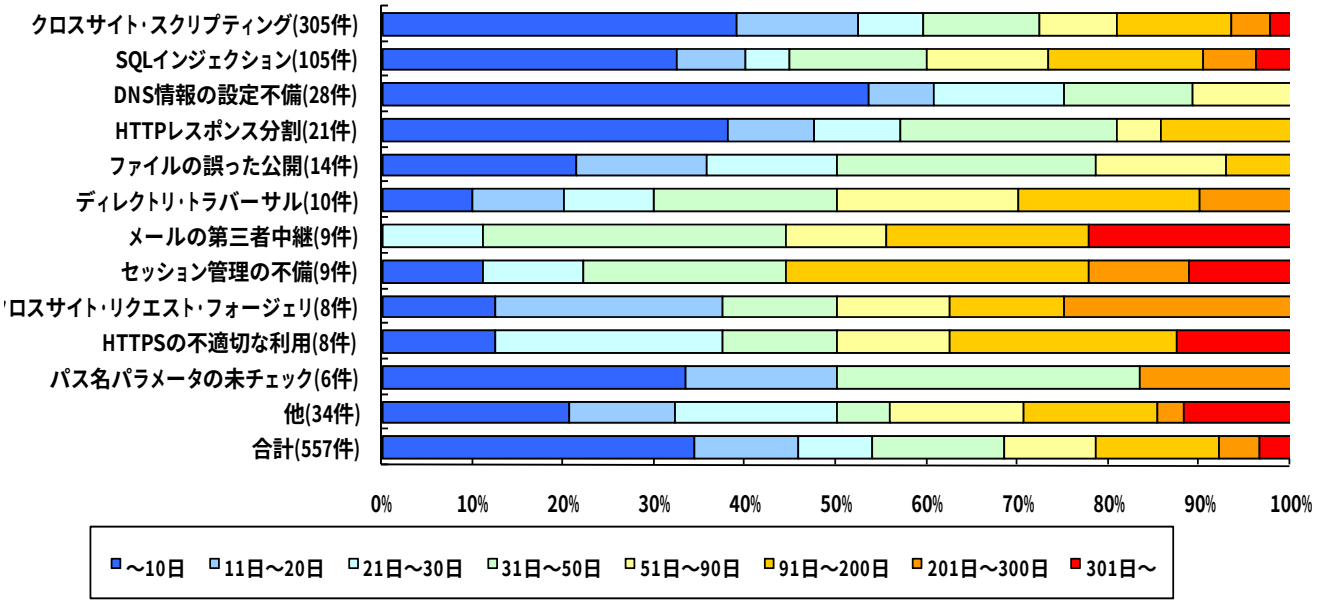


図 2-6.ウェブサイトの脆弱性修正に要した日数の傾向

参考

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

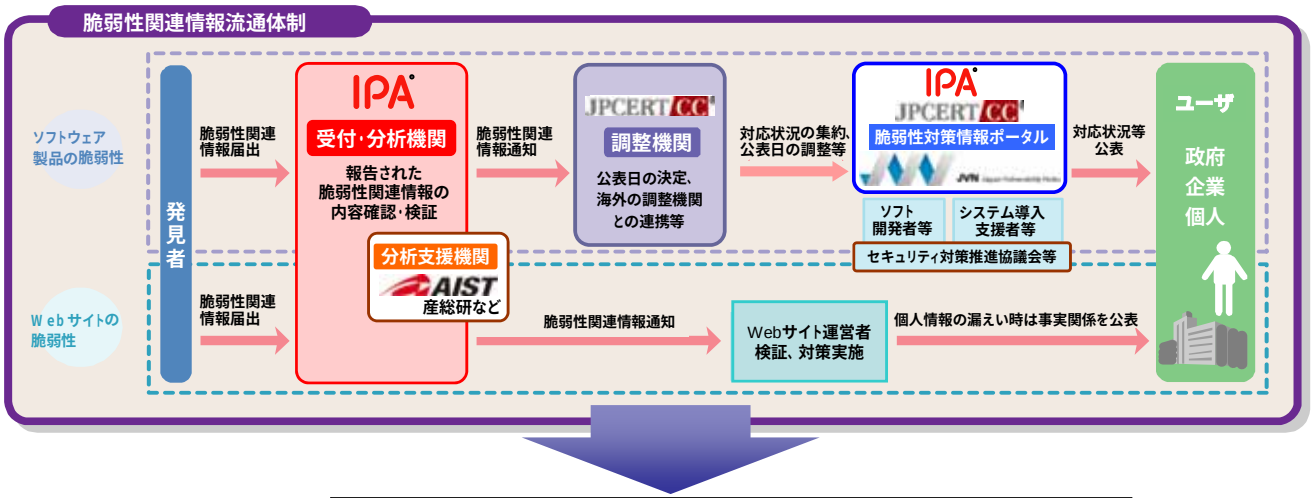
付表 2 ウェブサイト脆弱性の分類

	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