プレスリリース
2008 年 1 月 18 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 4 四半期(10 月～12 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 4 四半期(10 月～12 月)の脆弱性関連情報の届出状況[1]をまとめました。

今四半期のトピックス:
「情報セキュリティ早期警戒パートナーシップ」による脆弱性の修正完了件数が 1,000 件に達しました。

1. 2007 年第 4 四半期の概況

(1)脆弱性の届出状況

2007 年第 4 四半期(2007 年 10 月 1 日から 12 月 31 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 **66** 件、ウェブアプリケーション(ウェブサイト)に関するもの **80** 件、合計 **146** 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 **626** 件、ウェブサイトに関するもの **1,123** 件、合計 **1,749** 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)。

表 1. 2007 年第 4 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	66 件	626 件
ウェブサイト	80 件	1,123 件
計	146 件	1,749 件

図1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**業務日 1 日あたりの届出件数が、2007 年第 4 四半期で 2.05 件となりました。届出件数は年々増加しており、脆弱性の届出制度が浸透し、潜在していた脆弱性が顕在化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	2006/1Q	2006/2Q	2006/3Q	2006/4Q	2007/1Q	2007/2Q	2007/3Q	2007/4Q
1.45	1.61	1.70	1.75	1.92	1.95	1.98	2.03	2.05

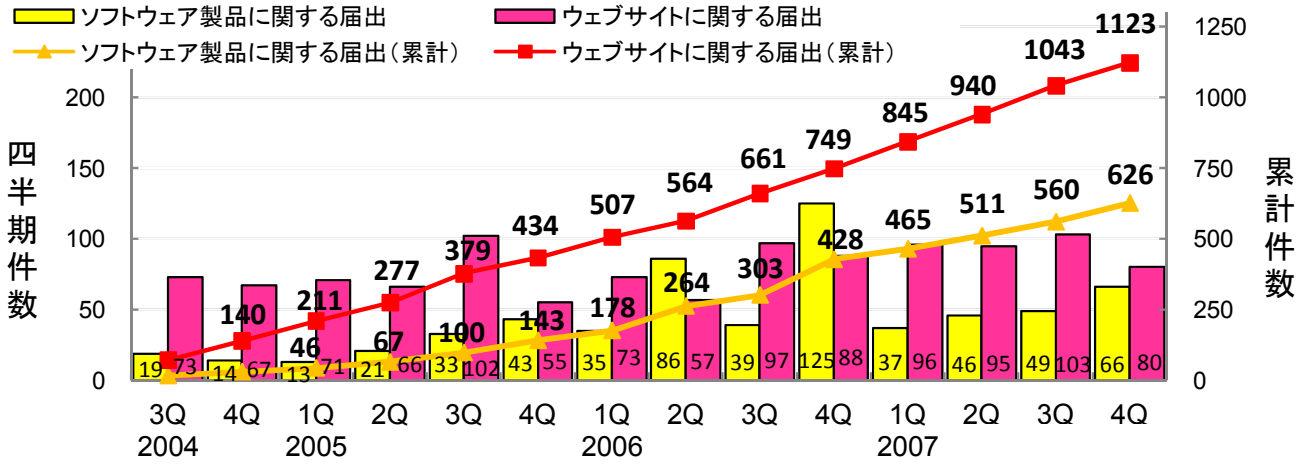


図 1. 脆弱性関連情報の届出件数の四半期別推移

[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。

(2)脆弱性の修正状況

2007 年第 4 四半期の脆弱性の修正完了件数は、ソフトウェア製品に関するもの **31** 件、ウェブサイトに関するもの **93** 件、合計 **124** 件でした。**届出受付開始からの累計は、ソフトウェア製品に関するもの 254 件、ウェブサイトに関するもの 748 件、合計 1,002 件となり、1,000 件に達しました**（表 2、図 2）。

表 2. 2007 年第 4 四半期の修正完了件数

分類	修正完了件数	累計件数
ソフトウェア製品	31 件	254 件
ウェブサイト	93 件	748 件
計	124 件	1,002 件

今四半期はソフトウェア製品の修正完了件数、ウェブサイトの修正完了件数ともに、過去最多となりました。

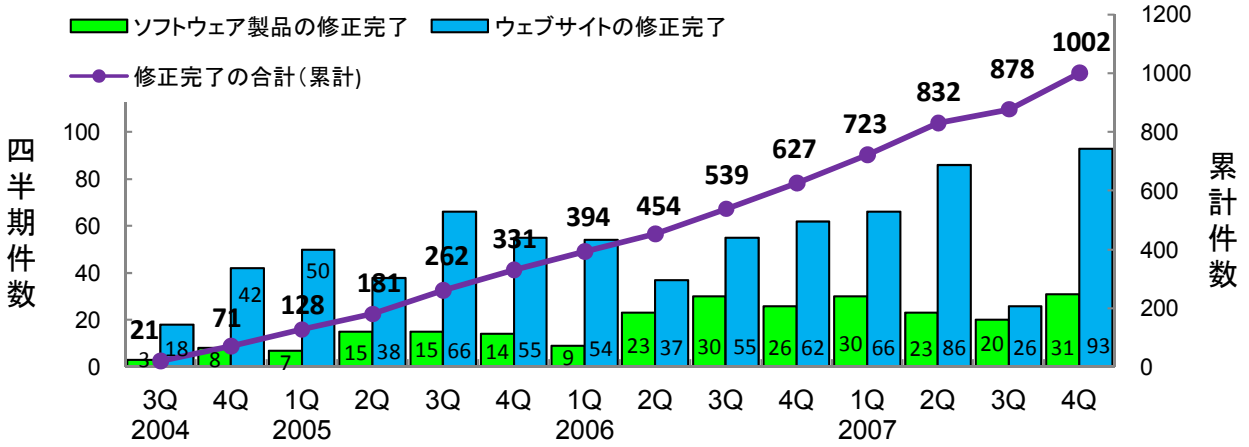


図 2. 脆弱性の修正完了件数の四半期別推移

修正が完了した脆弱性について、脆弱性を攻撃された場合に想定される脅威を分析すると、ソフトウェア製品の脆弱性に関しては、「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、「任意のスクリプトの実行」が **47%**、「情報の漏洩」が **10%**、「なりすまし」が **7%**、「任意のコードの実行」が **6%**などとなっています（図 3）。ウェブサイトの脆弱性に関しては、「本物サイトへの偽情報の表示」が **33%**、「データの改ざん、消去」が **18%**、「Cookie[2]情報の漏洩」が **16%**、「個人情報の漏洩」が **10%**などとなっています（図 4）。

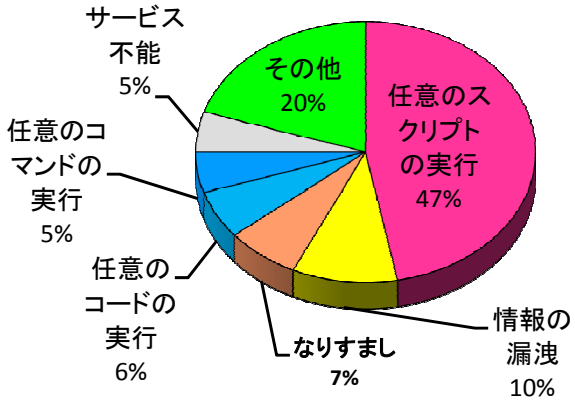


図 3. ソフトウェア製品の修正完了
－脅威別内訳－

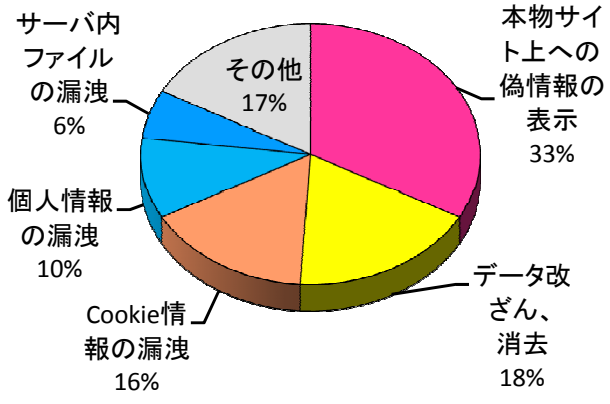


図 4. ウェブサイトの修正完了
－脅威別内訳－

IPA が 2006 年 11 月に公表した「企業における情報セキュリティ事象被害額調査」[3]によると、実際に SQL インジェクションによる不正アクセスがあった場合、その復旧に関する費用は 1 件あたり 5000 万円から 1 億円の推計結果となっています。**ソフトウェア製品開発者やウェブサイト運営者は、脆弱性対策を促進し、その被害を事前に防止することが重要です。**

---

[2] ウェブサイトの閲覧者のコンピュータに一時的にデータを書き込んで保存させるしくみ。Cookie には閲覧者の情報や最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができる。Cookie は閲覧者の識別に使われ、認証システムや、ウェブよるサービスを閲覧者ごとにカスタマイズするために利用される。

[3] http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html

2.ソフトウェア製品の脆弱性の処理状況

2007 年第 4 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 **31** 件でした。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は **0** 件、製品開発者が脆弱性ではないと判断したものは **2** 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 **8** 件でした。これらの取扱いを終了したものの合計は **41** 件（累計 **372** 件）です。この結果、取扱い中（製品開発者が調査、対応中のもの）が **25** 件増加し、**254** 件となりました（表 3）。

表 3. 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
修正完了	公表済み	31 件	242 件
	個別対応	0 件	12 件
脆弱性ではない		2 件	31 件
不受理		8 件	87 件
合計		41 件	372 件
取扱い中		25 件	254 件

今四半期のソフトウェア製品の脆弱性対策情報の公表件数は、31 件と過去最多となりました。このほか、海外の CSIRT[5]から JPCERT/CC が連絡を受けた 17 件（累計 303 件）を JVN で公表しました（図 5）。

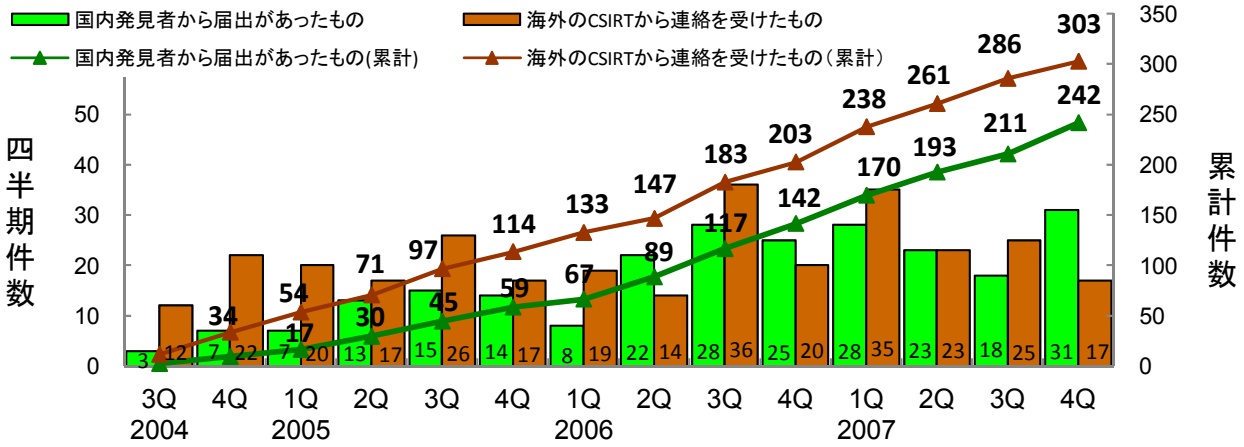


図５．ソフトウェア製品の脆弱性対策情報の公表件数の四半期別推移

なお、2007 年第 4 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)「一太郎シリーズ」の脆弱性[6]

日本語ワープロソフトの「一太郎シリーズ」の文書ファイルを読みこむ処理に、バッファオーバーフローの脆弱性が存在し、**ウェブブラウザの種類によっては、悪意のある URL にアクセスするだけで被害を受ける可能性がありました。**この脆弱性が悪用されると、システムが破壊されたり、ウイルスやボットに感染させられたりしてしまう可能性があり、10 月 25 日に JVN で対策情報を公表しました。

(2)「SonicStage CP」の脆弱性[7]

音楽管理ソフトウェアの「SonicStage CP」のプレイリストファイルを取り込む処理に、バッファオーバーフローの脆弱性が存在し、12 月 4 日に JVN で対策情報を公表しました。

本件は、**製品開発者自身から届出があり、JPCERT/CC が製品開発者と調整を行ない公表したものです。今後も、製品開発者に脆弱性対策情報を利用者へ周知徹底するための JVN の活用を求めます。**

(3)「Lhaplus」の脆弱性[8]

電子ファイルのデータを lzh 形式や zip 形式などに圧縮・解凍する Lhaplus に、バッファオーバーフローの

---

[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、別紙の表 1-2 項番 8 を参照下さい。

[7] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=6.8、別紙の表 1-2 項番 15 を参照下さい。

[8] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=6.8、別紙の表 1-2 項番 14 を参照下さい。

脆弱性が存在しました。この製品に関して、**前四半期に注意喚起を行いましたが、異なる個所に脆弱性があり、再度、11 月 22 日に JVN で対策情報を公表しました。**

また、類似の機能を持つソフトウェアの「PowerArchiver」「WinAce」にも同様の脆弱性が見つかっており、それぞれ 10 月 5 日、12 月 25 日に JVN で対策情報を公表しました。

(4) 「AirStation シリーズ」および「BroadStation シリーズ」の脆弱性[9]

ネットワーク機器の「AirStation シリーズ」および「BroadStation シリーズ」に組込まれたソフトウェアに、クロスサイト・リクエスト・フォージェリ(CSRF)の脆弱性があり、10 月 12 日に JVN で対策情報を公表しました。

(5) 「Webmin」の脆弱性[10]

OS のファイル編集やサーバ設定などを行えるようにするソフトウェアの「Windows 版 Webmin」に、OS コマンド・インジェクションの脆弱性が存在しました。この弱点が悪用されると、任意の OS コマンドが実行される可能性があり、10 月 3 日に JVN で対策情報を公表しました。

また、(4)のような組込みソフトウェアの脆弱性は、今四半期までに累計で 13 件公表しました(図 6)。対象となる組込み機器の内訳は、ルータやスイッチなどのネットワーク機器が **5** 件、プリンタやハードディスクなどの周辺機器が **3** 件、携帯電話が **3** 件、DVD レコーダなどの情報家電が **2** 件となっています(図 7)。

今後、情報家電がインターネットに接続されるようになると、組込みソフトウェアの脆弱性の顕著化が予測され、組込みソフトウェアの開発者は、製品の開発段階からセキュリティの考慮が必要です。

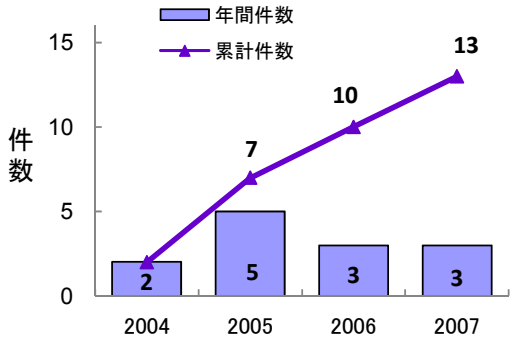


図6.組込みソフトウェアの脆弱性の修正完了件数の年別推移

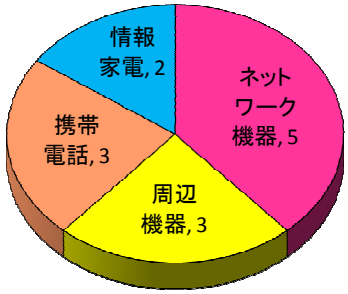


図7.組込みソフトウェアの脆弱性の対象機器

これらのソフトウェア製品の脆弱性の処理状況の詳細は別紙の 1 章を参照下さい。

3.ウェブサイトの脆弱性の処理状況

2007 年第 4 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 **93** 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 **20** 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 **4** 件でした。これらの取扱いを終了したものの合計は **117** 件(累計 **962** 件)です。この結果、取扱い中(ウェブサイト運営者が調査、対応中のもの)のものが **37** 件減少し、**161** 件となりました(表 4)。

表 4. 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	93 件	748 件
脆弱性ではない	20 件	131 件
連絡不可能	0 件	7 件
不受理	4 件	76 件
合計	117 件	962 件
取扱い中	−37 件	161 件

今四半期のウェブサイトの脆弱性の修正完了件数は、93 件と過去最多となりました(図 8)。

[9] 本脆弱性の深刻度=レベル II(警告)、CVSS 基本値=4.0、別紙の表 1-2 項番 4 を参照下さい。
[10] 本脆弱性の深刻度=レベル III(危険)、CVSS 基本値=9.0、別紙の表 1-2 項番 1 を参照下さい。

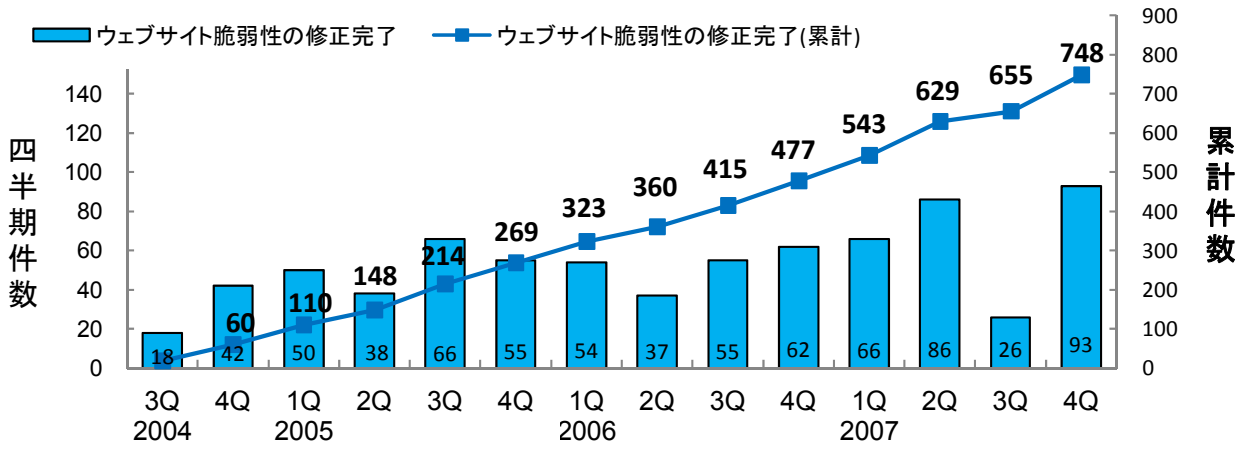


図８. ウェブサイトの脆弱性の修正完了件数の四半期別推移

(1) 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が 95 件となりました

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、1～2 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。

今四半期は修正が長期化しているウェブサイトに対し、脆弱性が攻撃された場合の具体的な脅威を丁寧に解説するなど、特に重点的に脆弱性対策を促しました。この結果、図 9 に示すように、90 日以上も対策が完了していないものが前四半期から **22** 件減少し **95** 件（前四半期は **117** 件）となりました。

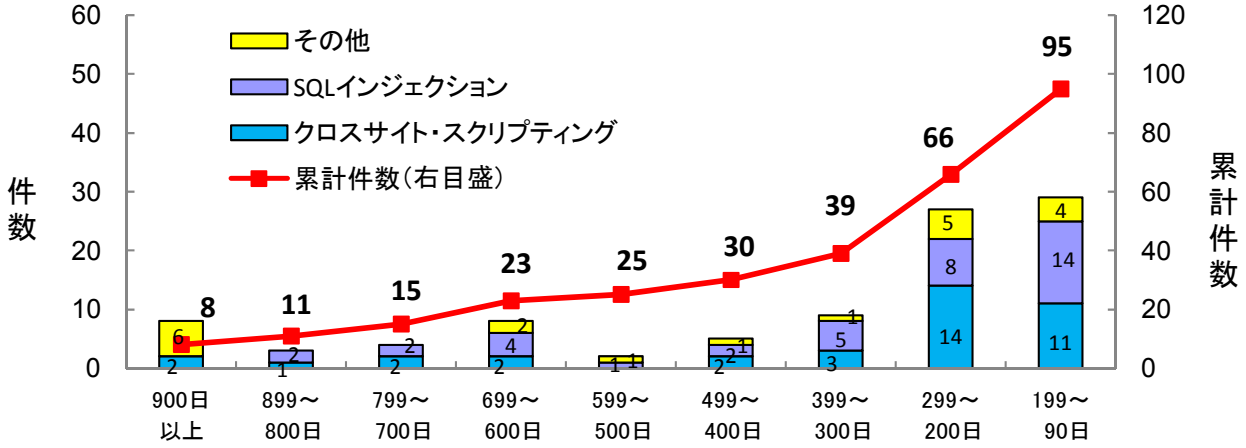


図9.修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

なお、300 日以上も対策が完了していないものが、**39** 件（前四半期は **50** 件）あります。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が必要があります。**

これらのウェブサイトの脆弱性の処理状況の詳細は、別紙の 2 章を参照下さい。

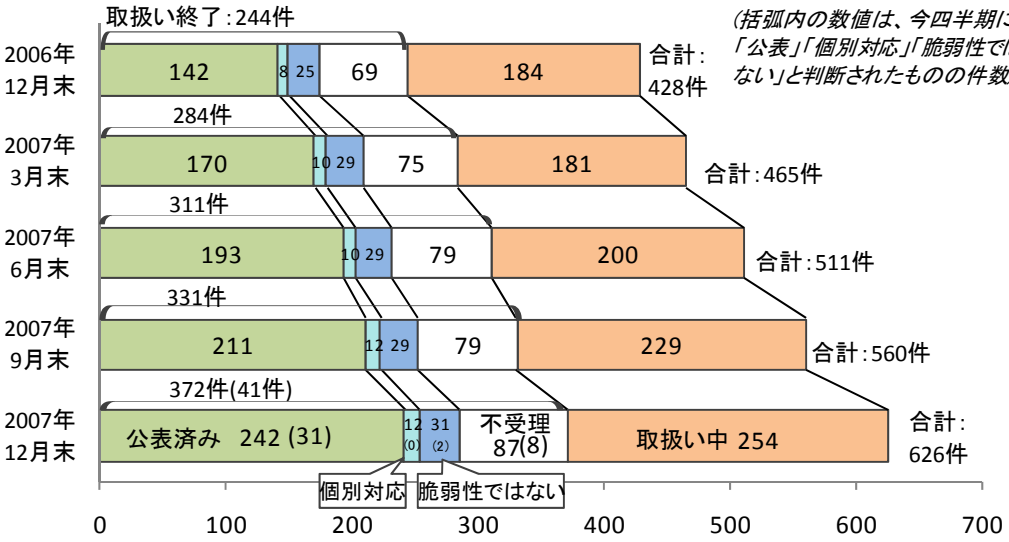
■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: office@jpcert.or.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503 Fax:03-5978-7510 E-mail: pr-inq@ipa.go.jp
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. 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、**31** 件（累計 **242** 件）です。また、「不受理」としたものは **8** 件（累計 **87** 件）です。



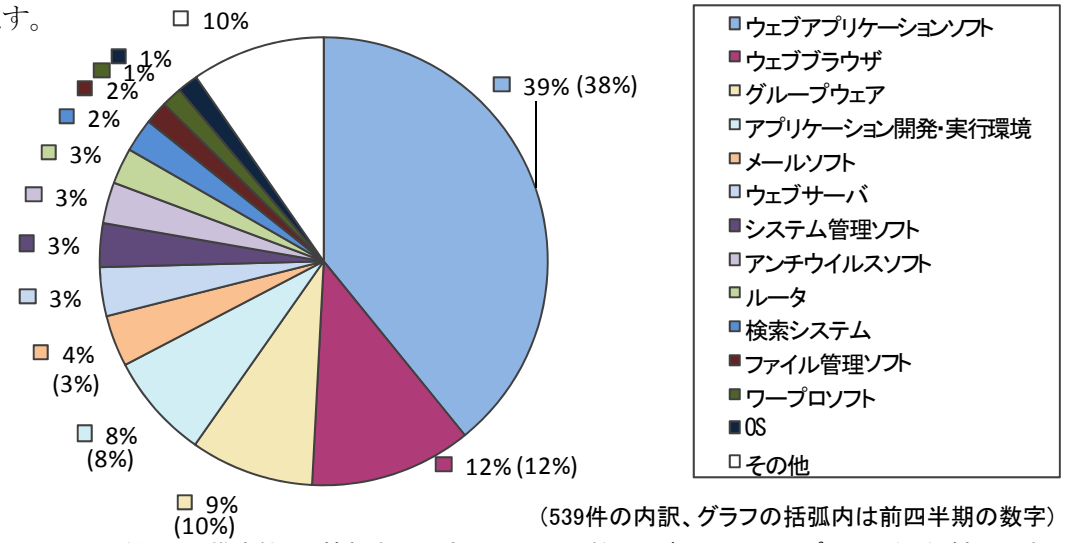
公表済み:	JVN で脆弱性への対応状況を公表したもの
個別対応:	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない:	製品開発者により脆弱性ではないと判断されたもの
不受理:	告示で定める届出の対象に該当しないもの
取扱い中:	製品開発者が調査、対応中のもの

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 **626** 件のうち、不受理のものを除いた **539** 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。



(539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2007年12月末まで）

図 1-3 に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 10 件の届出がありました。

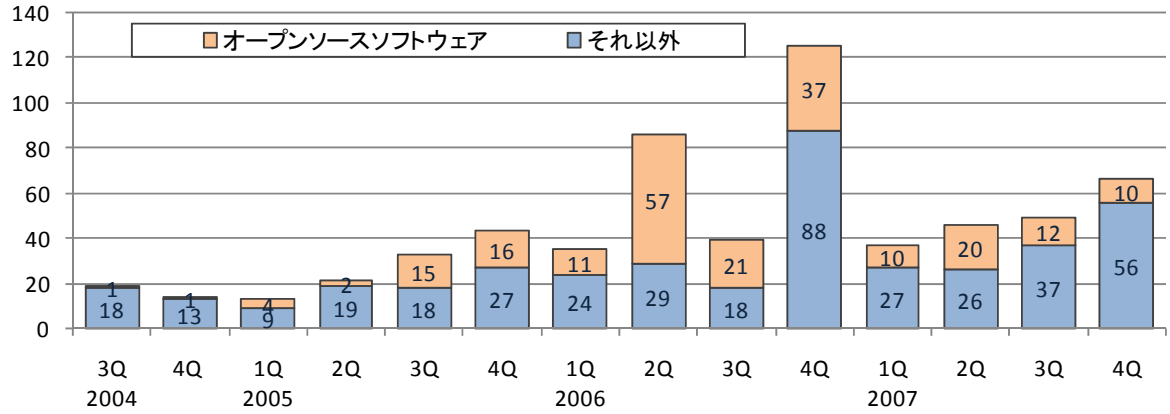
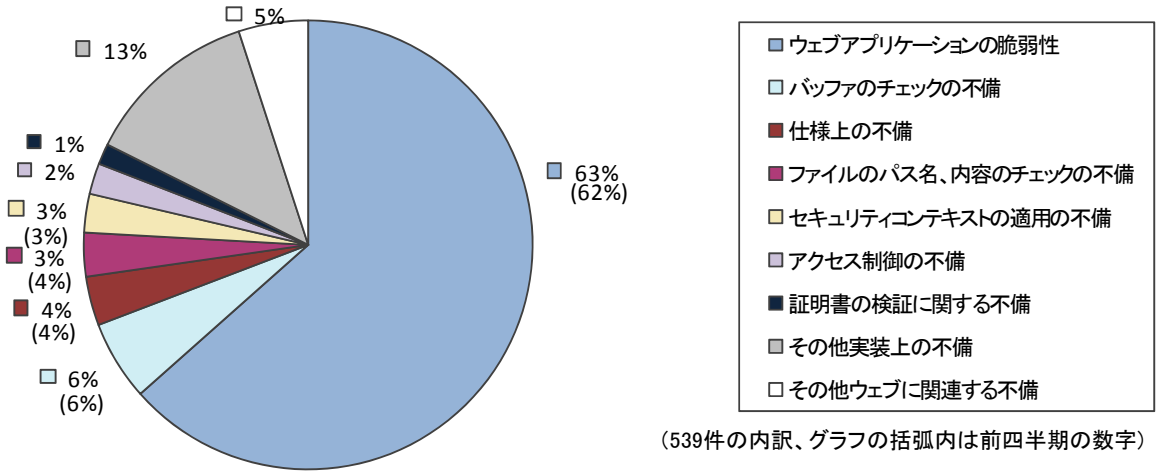


図1-3.オープンソースソフトウェアの脆弱性の届出件数

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 **626** 件のうち、不受理のものを除いた **539** 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 3 年以上も続いています。



（539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2007年12月末まで）

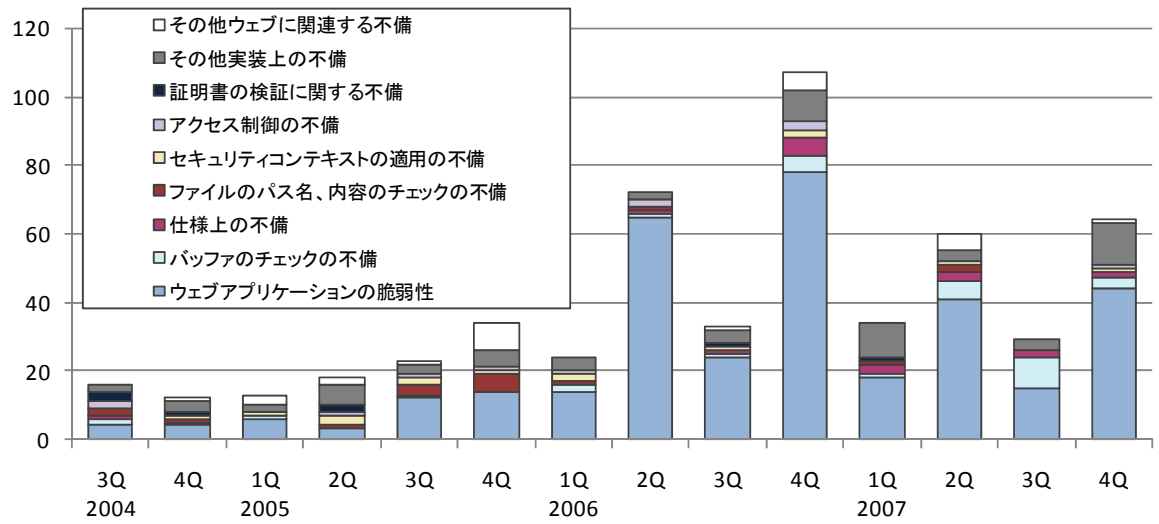
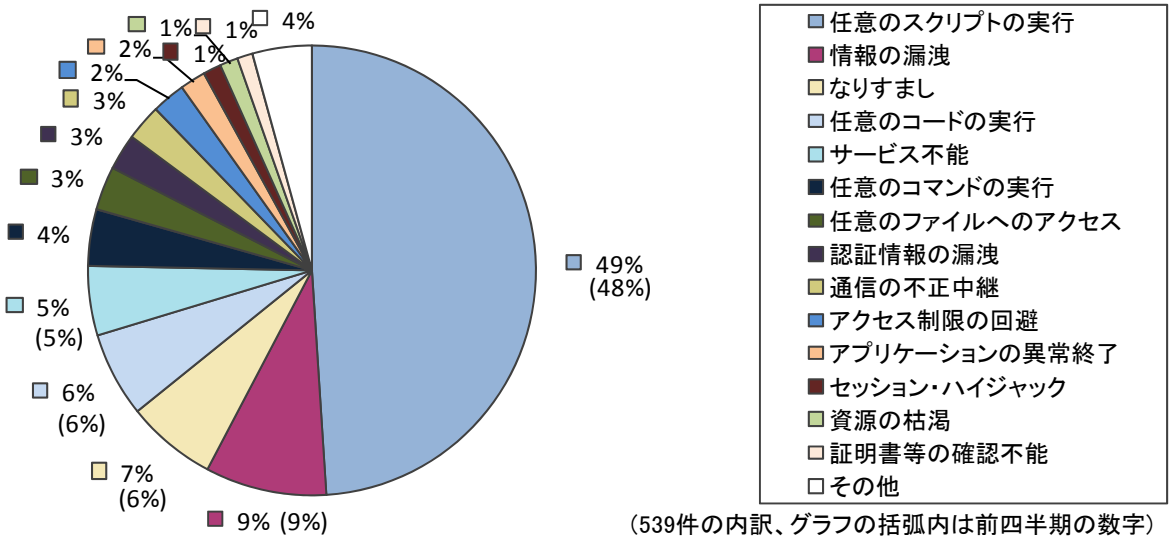


図1-5. ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2007年12月末まで）



（539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2007年12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[11] 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	31 件	242 件
②	海外 CSIRT 等と連携して公表したもの	17 件	303 件
	計	48 件	545 件

[11] 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 2007 年 12 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 34%と減少し、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。

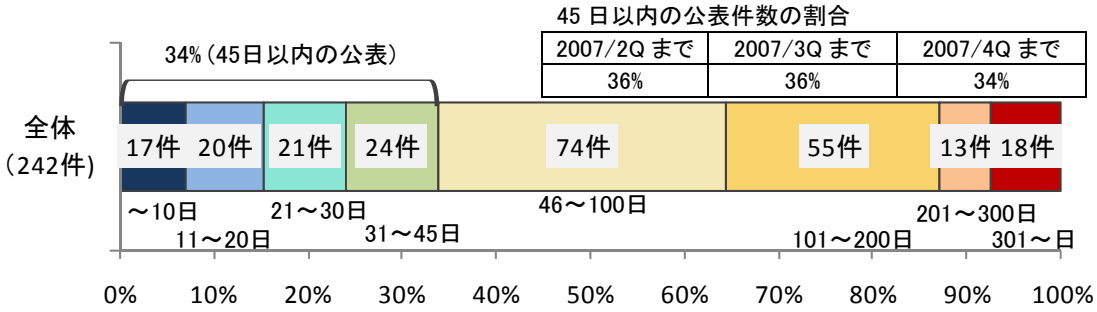


図1-7. ソフトウェア製品の脆弱性 公表日数

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 7 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 2 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）あり、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 4 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 III（危険）、CVSS 基本値=7.0～10.0				
1	Webmin における OS コマンド・インジェクションの脆弱性	ウェブベースのシステム管理ツール「Webmin」には、利用者からの入力の処理に問題がありました。このため、Webmin を設置しているコンピュータにおいて、ローカルシステム権限で任意の OS コマンドを実行される可能性がありました。	2007 年 10 月 3 日	9.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
2	Safari において HTTP 通信のページから HTTPS 通信のページにアクセス可能な脆弱性	Apple 製ウェブブラウザ「Safari」には、HTTPS 通信により保護されているページの内容が、同じドメインの保護されていない HTTP 通信のページからアクセス可能な脆弱性が存在しました。このため、HTTPS 通信で保護されているページの内容が、同じドメインの HTTP 通信のページから取得、変更される可能性がありました。	2007 年 10 月 1 日	4.0
3	PowerArchiver 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「PowerArchiver」には、バッファオーバーフローの脆弱性が存在しました。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した。	2007 年 10 月 5 日	6.8
4 (*4)	AirStation シリーズおよび BroadStation シリーズ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	バッファロー製ルータである「AirStation シリーズ」および「BroadStation シリーズ」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存在しました。ウェブ設定画面にログインした状態で悪意あるページにアクセスした場合、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。	2007 年 10 月 12 日	4.0

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
5 (*1)	MouseoverDictionary において任意のスクリプトが実行される脆弱性	Mozilla Firefox 用の拡張機能ソフト「MouseoverDictionary」には、サイドバーに HTML ページを出力する際の処理に問題がありました。このため、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した。	2007 年 10 月 12 日	5.8
6	一太郎シリーズにバッファオーバーフローの脆弱性	ジャストシステムが提供する「一太郎シリーズ」には、バッファオーバーフローの脆弱性が存在しました。7,8 で修正された問題とは異なります。このため、ウェブサイト等でファイルを見るだけで、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した。	2007 年 10 月 25 日	6.8
7	一太郎シリーズにバッファオーバーフローの脆弱性	ジャストシステムが提供する「一太郎シリーズ」には、バッファオーバーフローの脆弱性が存在しました。6,8 で修正された問題とは異なります。このため、ウェブサイト等でファイルを見るだけで、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した。	2007 年 10 月 25 日	6.8
8	一太郎シリーズにバッファオーバーフローの脆弱性	ジャストシステムが提供する「一太郎シリーズ」には、バッファオーバーフローの脆弱性が存在しました。6,7 で修正された問題とは異なります。このため、ウェブサイト等でファイルを見るだけで、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した。	2007 年 10 月 25 日	6.8
9 (*1)	NetCommons 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「NetCommons」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。	2007 年 11 月 5 日	4.3
10	Lotus Domino 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「Lotus Domino」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。	2007 年 11 月 7 日	4.3
11	UPDIR.NET 製 updir.php におけるクロスサイト・スクリプティングの脆弱性	画像ファイル管理ソフト「UPDIR.NET 製 updir.php」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。	2007 年 11 月 9 日	4.3
12 (*1)	Feed2JS におけるクロスサイト・スクリプティングの脆弱性	RSS データを JavaScript に変換するソフト「Feed2JS」には、JavaScript プログラムの出力に、任意の JavaScript を埋めこめる問題がありました。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。	2007 年 11 月 20 日	4.3
13	FileMaker におけるクロスサイト・スクリプティングの脆弱性	データベースソフト「FileMaker」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。	2007 年 11 月 21 日	4.3
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した。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した。	2007 年 11 月 22 日	6.8

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
15 (*2)	SonicStage CP におけるバッファオーバーフローの脆弱性	音楽管理ソフト「SonicStage CP」には、バッファオーバーフローの脆弱性が存在しました。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した。	2007 年 12 月 4 日	6.8
16	サイボウズ Office におけるサービス運用妨害(DoS)の脆弱性	グループウェア「サイボウズ Office」には、HTTP リクエストを処理する際にサーバリソースを過剰に消費する問題がありました。このため、サーバの処理速度が極端に低下し、サービス不能状態になる可能性がありました。	2007 年 12 月 11 日	4.3
17	複数のサイボウズ製品におけるクロスサイト・スクリプティングの脆弱性	複数のサイボウズ製品には、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。19 で修正された問題とは異なります。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した。	2007 年 12 月 11 日	4.3
18	複数のサイボウズ製品における HTTP ヘッダインジェクションの脆弱性	複数のサイボウズ製品には、HTTP ヘッダを出力する際の処理に問題がありました。このため、第三者によりウェブページに偽の情報が表示される可能性や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した。	2007 年 12 月 11 日	4.3
19	複数のサイボウズ製品におけるクロスサイト・スクリプティングの脆弱性	複数のサイボウズ製品には、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。17 で修正された問題とは異なります。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した。	2007 年 12 月 11 日	4.3
20	Rainboard におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフト「Rainboard」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。	2007 年 12 月 12 日	4.3
21	JP1/Cm2/Network Node Manager におけるクロスサイト・スクリプティングの脆弱性	ネットワーク管理ソフト「JP1/Cm2/Network Node 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。	2007 年 12 月 13 日	4.3
22 (*1) (*3)	Apache HTTP Server の mod_imap および mod_imagemap におけるクロスサイト・スクリプティングの脆弱性	Apache HTTP Server のサーバサイドイメージマップ処理モジュール「mod_imap」および「mod_imagemap」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。	2007 年 12 月 13 日	4.3
23	Flash Player において任意の HTTP 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 HTTP ヘッダが送信可能な問題がありました。このため、HTTP 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した。	2007 年 12 月 20 日	4.3

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
24	Sun Java System Web Server および Sun Java System Web Proxy Server におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバ「Sun Java System Web Server」および「Sun Java System Web Proxy Server」には、ログ閲覧機能にクロスサイト・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。	2007 年 12 月 21 日	4.3
25	WinAce 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「WinAce」には、バッファオーバーフローの脆弱性が存在しました。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した。	2007 年 12 月 25 日	6.8
26 (*1) (*2)	GreaseKit および Creammonkey における許可されていない関数が実行される脆弱性	Apple Webkit 用拡張機能ソフト「GreaseKit」および「Creammonkey」には、本来ウェブページ上のスクリプトから許可されていない関数が実行できる問題がありました。このため、第三者により任意のサイトへ HTTP リクエストを送信されたり、ユーザスクリプトの設定値の読み書きが行われたりする可能性がありました。	2007 年 12 月 26 日	4.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
27	Sleipnir および Grani のお気に入り検索機能において任意のスクリプトが実行される脆弱性	ウェブブラウザ「Sleipnir」および「Grani」には、お気に入り機能の検索結果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、意図しないスクリプトが実行される可能性がありました。	2007 年 11 月 13 日	2.6
28 (*1)	RoundCube Webmail 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	ウェブメールソフト「RoundCube Webmail」には、クロスサイト・リクエスト・フォージェリの脆弱性が存在しました。このため、メールの件名などの一部情報が漏えいする可能性がありました。	2007 年 11 月 19 日	2.6
29	HttpLogger におけるクロスサイト・スクリプティングの脆弱性	ウェブページの閲覧履歴全文検索ソフト「HttpLogger」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。	2007 年 12 月 7 日	4.3
30 (*1)	Google Web Toolkit 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のためのフレームワーク「Google Web Toolkit」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。	2007 年 12 月 18 日	2.6
31	Flash Player におけるクロスドメインポリシーファイルの扱いに関する脆弱性	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、クロスドメインポリシーファイルの扱いに問題がありました。このため、クロスドメインポリシーで許可していないウェブページにアクセスされる可能性がありました。	2007 年 12 月 20 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 25 件には、通常の脆弱性情報 6 件(表 1-3)と、対応に緊急を要する Technical Cyber Security Alert(表 1-4)の 11 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[12]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	JRE(Java Runtime Environment)に遠隔の第三者がネットワークリソースへ接続可能な脆弱性	複数製品開発者へ通知
2	CUPS 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
3	Mozilla Firefox における jar URI にクロスサイト・スクリプティングの脆弱性	注意喚起として掲載
4	Apple QuickTime RTSP の Content-Type ヘッダの処理にスタックバッファオーバーフローの脆弱性	緊急案件として掲載
5	Apple Mail 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
6	ジャストシステム製品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

表 1-4.米国 US-CERT[13]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 製品における複数の脆弱性
2	Oracle 製品に複数の脆弱性
3	Microsoft Windows における URI 処理の脆弱性に対する Adobe 製品のアップデート
4	リアルネットワークス RealPlayer におけるプレイリストの処理にバッファオーバーフローの脆弱性
5	Apple QuickTime に複数の脆弱性
6	Microsoft 製品における複数の脆弱性
7	Apple の Mac 製品に複数の脆弱性
8	Apple QuickTime の RTSP 処理にバッファオーバーフローの脆弱性
9	Microsoft 製品における複数の脆弱性
10	Apple 製品における複数の脆弱性
11	Adobe Flash player における複数の脆弱性に対するアップデート

[12] CERT/Coordination Center。1998 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。
[13] 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 **117** 件（累計 **962** 件）でした。このうち、「修正完了」したものは **93** 件（累計 **748** 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 **20** 件（累計 **131** 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 **4** 件（累計 **76** 件）でした。

取扱いを終了した累計 **962** 件のうち、「連絡不可能」「不受理」を除く累計 **879** 件（**91**%）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 **11** 件（累計 **124** 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 **6** 件（累計 **68** 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 **1** 件（累計 **19** 件）でした。

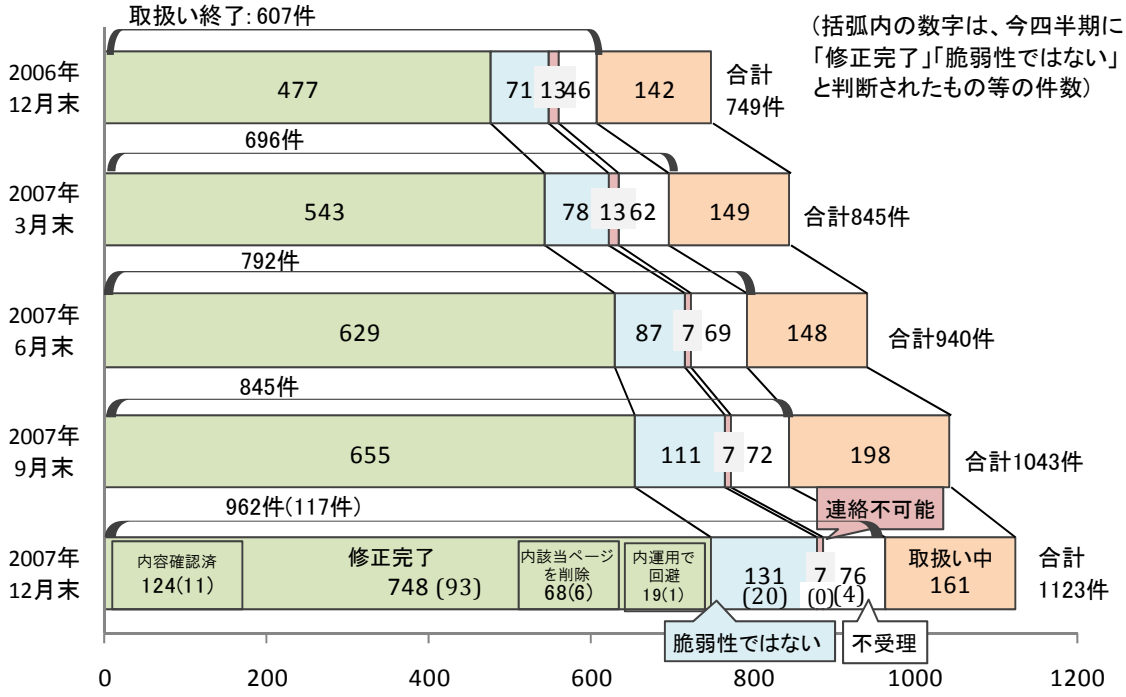
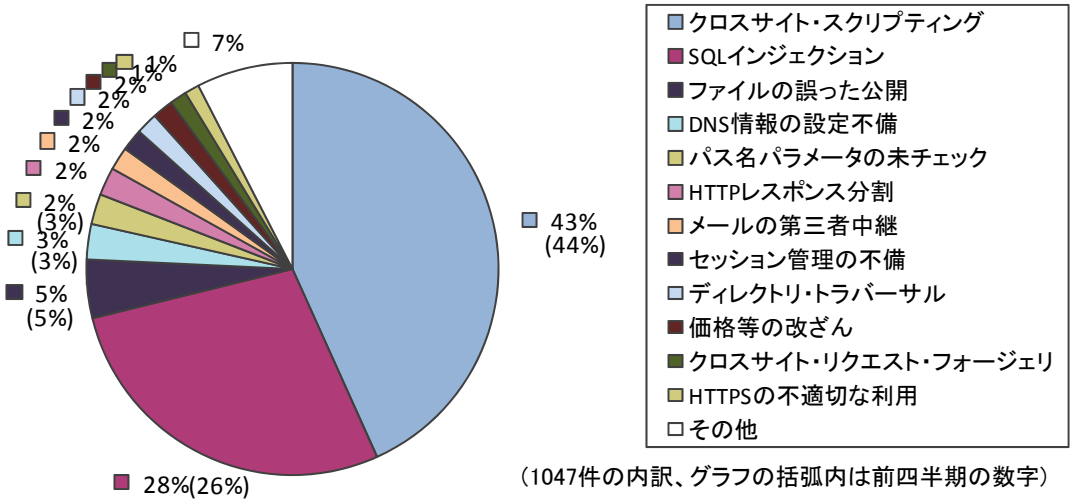


図 2-1.ウェブサイト各時点における脆弱性関連情報の届出の処理状況

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
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

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 **1,123** 件のうち、不受理のものを除いた **1,047** 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[14]。



（1047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12月末まで）

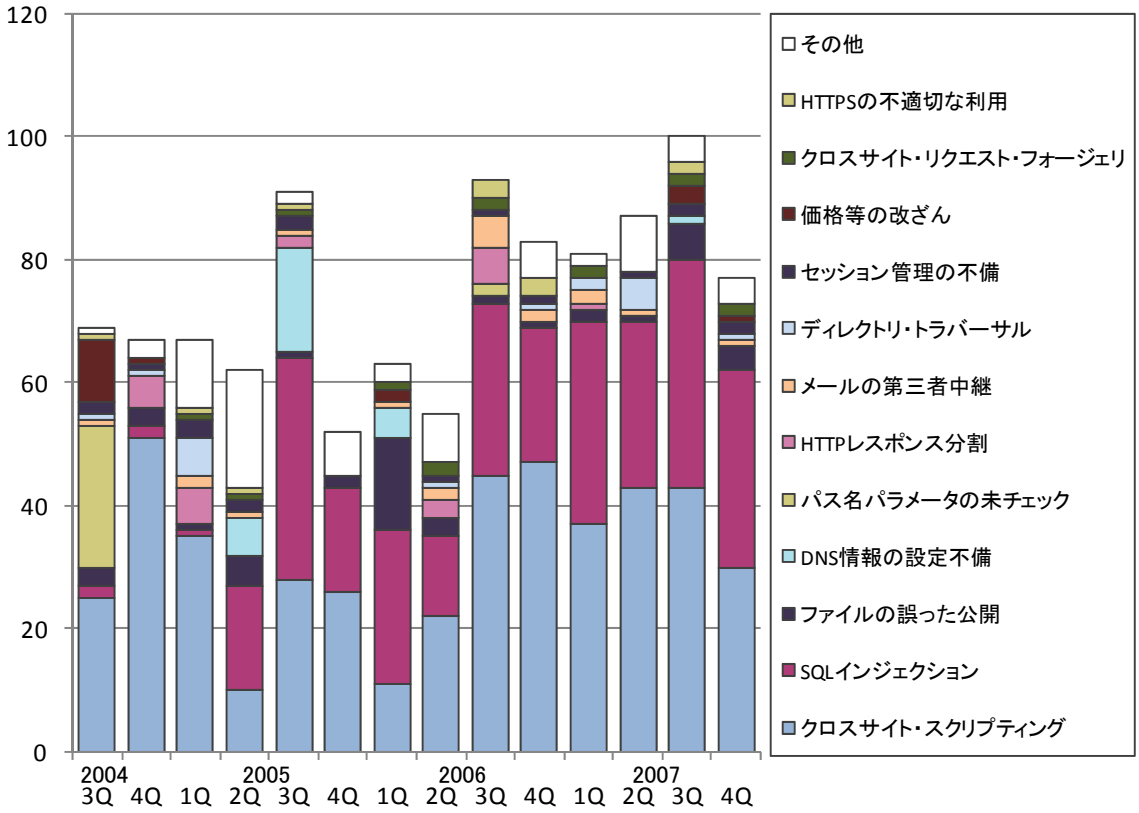
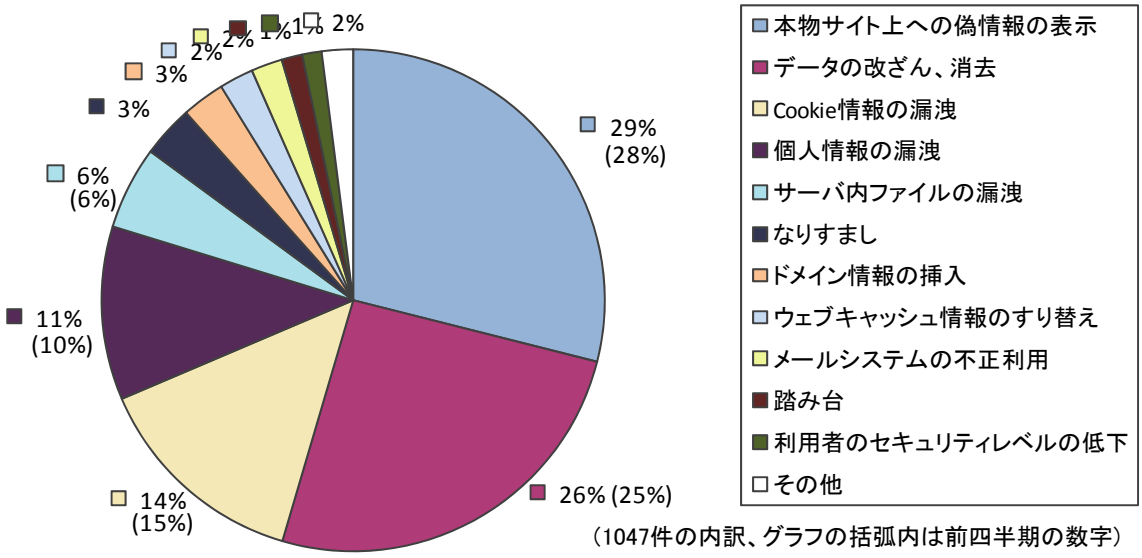


図2-3.ウェブサイトの脆弱性 種類別件数の推移（届出受付開始から2007年12月末まで）

[14] 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。



（1047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12月末まで）

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、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 2007 年 12 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 53%の届出が 30 日以内、全体の 78%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

2007/2Q まで	2007/3Q まで	2007/4Q まで
79%	79%	78%

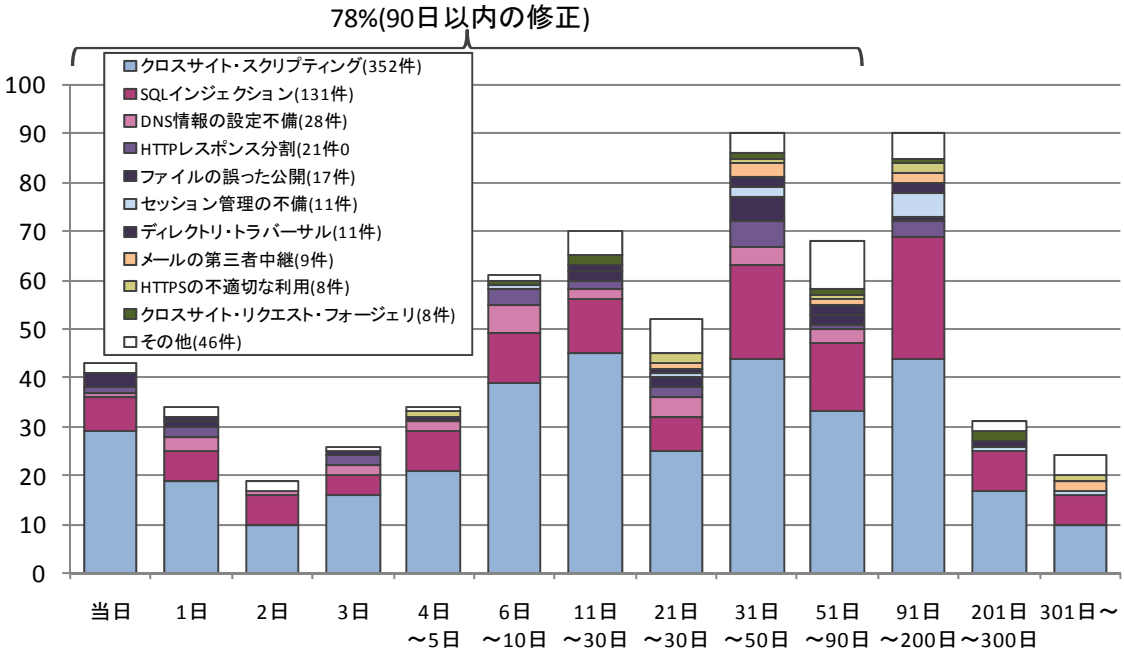


図2-5.ウェブサイトの修正に要した日数

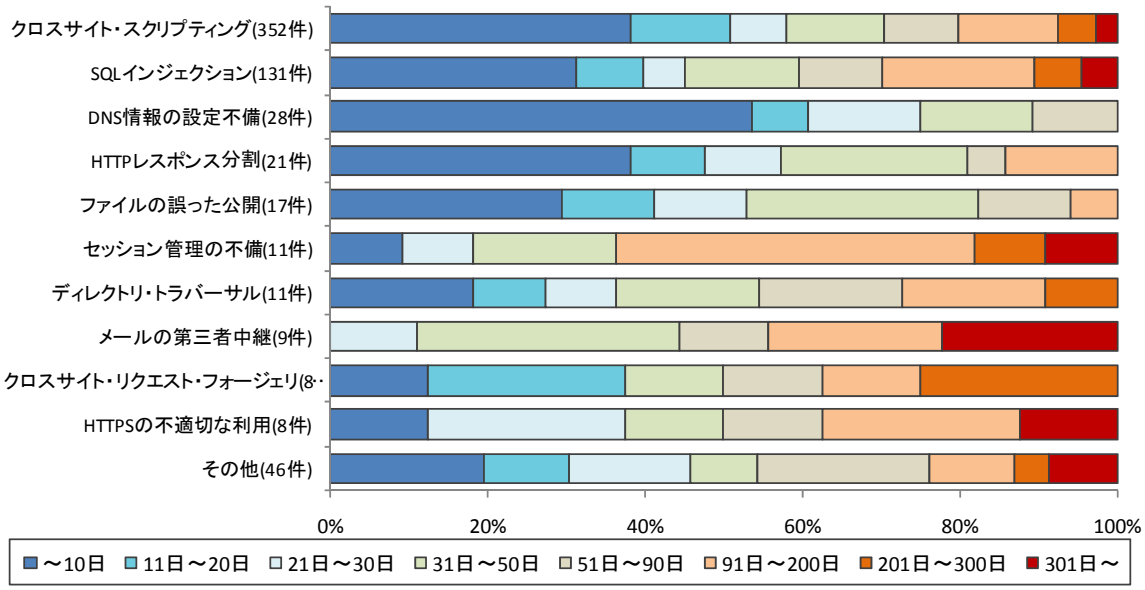


図2-6.ウェブサイトの修正に要した日数の傾向

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、セキュリティ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/

(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。

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

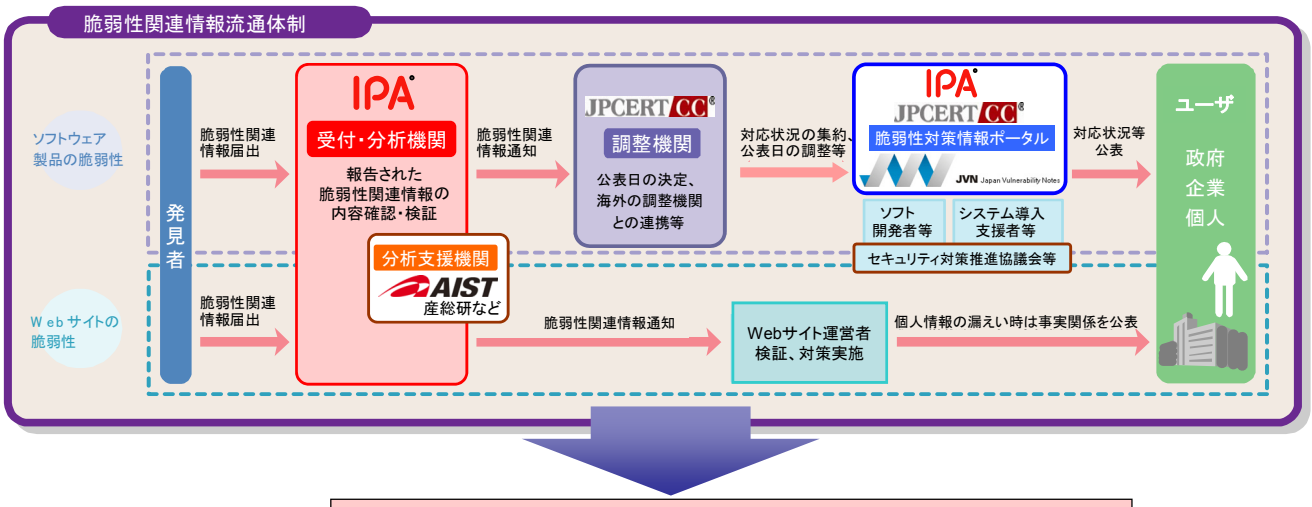
付表 2 ウェブサイト脆弱性の分類

	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
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

	脆弱性の種類	深刻度	説明	届出において想定された脅威
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