Information-technology Promotion Agency, Japan

JPCERT CC®

プレスリリース

2011 年 10 月 21 日
独立行政法人情報処理推進機構
一般社団法人 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 [2011 年第 3 四半期（7 月～9 月）]

～ウェブサイトに関する脆弱（ぜいじゃく）性関連情報の届出が前四半期の 5 倍に～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）および JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター、代表理事：歌代 和正）は、 2011 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。

（1）脆弱性の届出件数の累計が 6,891 件に（別紙 1　1.参照）

2011 年第 3 四半期の IPA への脆弱性関連情報の届出件数は 234 件です。内訳は、ソフトウェア製品に関するものが 36 件、ウェブアプリケーション （ウェブサイト）に関するものが 198 件でした。これにより、2004 年 7 月の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が 1,249 件、ウェブサイトに関するものが 5,642 件、合計 6,891 件となりました。

今四半期のウェブサイトに関する届出は、前四半期の 5 倍以上となりました。なお、その 9 割はクロスサイト・スクリプティングの脆弱性に関するものです。

（2）脆弱性の修正完了件数の累計が 4,100 件を突破（別紙 1　2.参照）

ソフトウェア製品の脆弱性の届出に関して、JPCERT/CC が調整を行い、製品開発者が修正を完了し、2011 年第 3 四半期に JVN 対策情報を公表したものは 29 件（累計 545 件）でした。また、ウェブサイトの脆弱性の届出に関して、IPA がウェブサイト運営者に通知し、2011 年第 3 四半期に修正を完了したものは 86 件（累計 3,596 件）でした。これにより、ソフトウェア製品を含めた脆弱性の修正件数は累計で 4,141 件となりました。

（3）届出をする発見者が所属する組織に変化（別紙 1　4.参照）

これまで、脆弱性関連情報の発見者のほとんどは企業または個人でしたが、2011 年は 9 月末時点で大学や高校などの教育・学術機関からの届出が約半数を占める傾向に変化してきています（発見者の自己申告情報による集計結果）。今後もより多くの方からの届出を期待しています。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 渡辺／大森
Tel: 03-5978-7527　Fax: 03-5978-7518
E-mail: vuln-inq@ipa.go.jp
JPCERT/CC 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
IPA 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
JPCERT/CC 事業推進基盤グループ 広報 江田
Tel: 03-3518-4600　Fax: 03-3518-4602
E-mail: pr@jpcert.or.jp

(*1) ソフトウェア等脆弱性関連情報取扱基準：経済産業省告示（http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf）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。

別紙 1

2011 年第 3 四半期　ソフトウェア等の脆弱性関連情報に関する届出状況（総括）

1.脆弱性関連情報の届出状況

～ 脆弱性の届出件数の累計が 6,891 件になりました ～

表 1 は 2011 年第 3 四半期の IPA への脆弱性関連情報の届出件数および届出開始（2004 年 7 月 8 日）から今四半期までの累計件数を示しています。今期の届出件数はソフトウェア製品に関するもの 36 件、ウェブアプリケーション（ウェブサイト）に関するもの 198 件、合計 234 件でした。

表 1.　届出件数

分類	今期件数	累計件数
ソフトウェア製品	**36** 件	**1,249** 件
ウェブサイト	**198** 件	**5,642** 件
合計	**234** 件	**6,891** 件

届出受付開始からの累計件数は、ソフトウェア製品に関するもの 1,249 件、ウェブサイトに関するもの 5,642 件、合計 6,891 件となりました。ウェブサイトに関する届出が全体の 82%を占めています。

図 1 のグラフは過去 3 年間の届出件数の四半期別推移を示したものです。今四半期のソフトウェア製品の届出は前四半期と比較して減少しましたが、ウェブサイトの届出が急増し前四半期の 5 倍強となっています。表 2 は過去 3 年間の四半期別の累計届出件数および 1 就業日あたりの届出件数の推移です。1 就業日あたりの届出件数は 2011 年第 3 四半期末で 3.91(*1)件となりました。

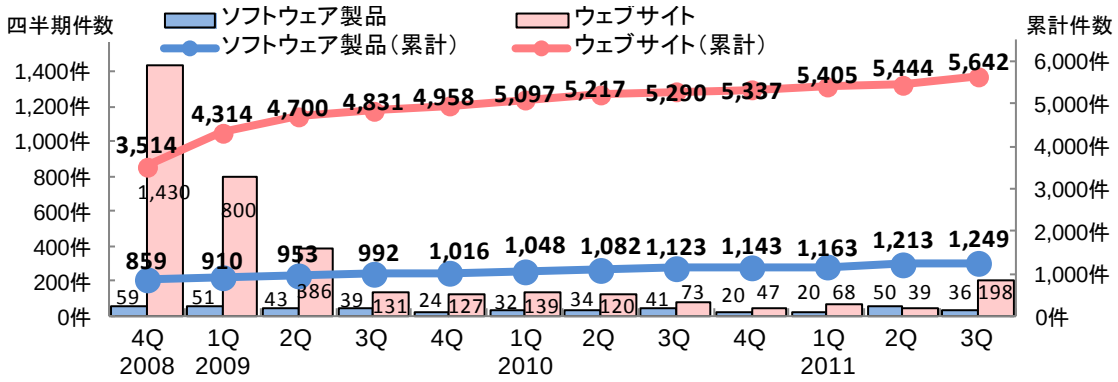


図 1.脆弱性関連情報の届出件数の四半期別推移

表 2. 届出件数（過去 3 年間）

	2008 4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q
累計届出件数[件]	4,373	5,224	5,653	5,823	5,974	6,145	6,299	6,413	6,480	6,568	6,657	6,891
1就業日あたり[件/日]	3.99	4.53	4.65	4.56	4.47	4.40	4.32	4.22	4.10	4.00	3.92	3.91

図 2 のグラフは今四半期に届出されたソフトウェア製品の脆弱性関連情報 36 件のうち、不受理を除いた 35 件の製品種類の内訳を、図 3 は脆弱性がもたらす脅威の内訳を示したものです。製品の種類は「ウェブアプリケーションソフト」が最も多く、次いで「ウェブブラウザ」と「OS」となっています。脆弱性がもたらす脅威は「任意のスクリプト実行」、「情報漏洩」、「サービス不能」が多く届出されており、これらの届出で全体の 6 割を占めています。

(*1)　1 就業日あたりの届出件数は、「累計届出件数」/「届出受付開始からの就業日数」にて算出

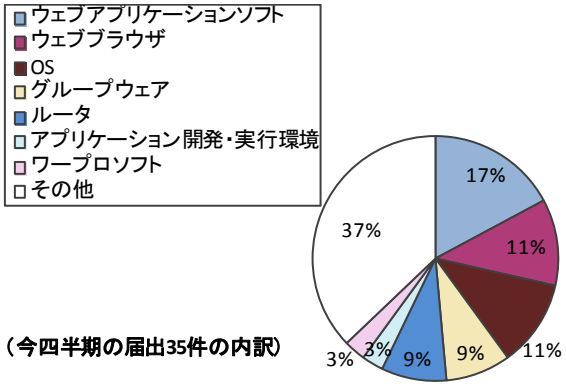


図2. 今四半期のソフトウェア製品種類の内訳

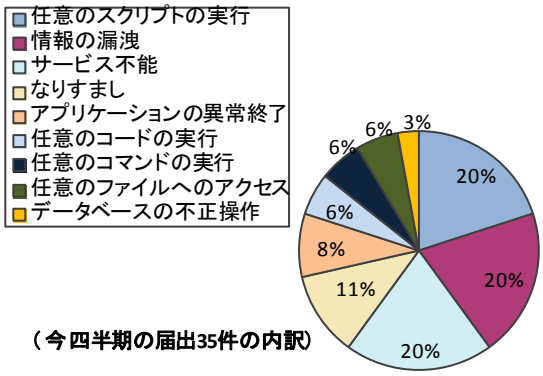


図3. 今四半期の脆弱性がもたらす脅威の内訳

図 4 のグラフは今四半期に届出されたウェブサイトの脆弱性関連情報 198 件のうち、不受理を除いた 194 件のウェブサイト運営主体の内訳を、図 5 は脆弱性の種類の内訳を示したものです。運営主体は「企業」が全体の 77%を占めています。また、脆弱性の種類は「クロスサイト・スクリプティング」が最も多く、全体の 92%を占めています。

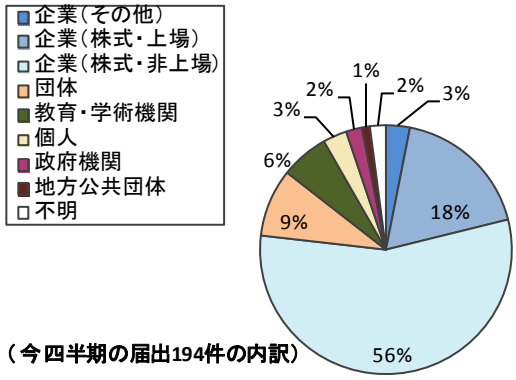


図4. 今四半期のウェブサイト運営主体の内訳

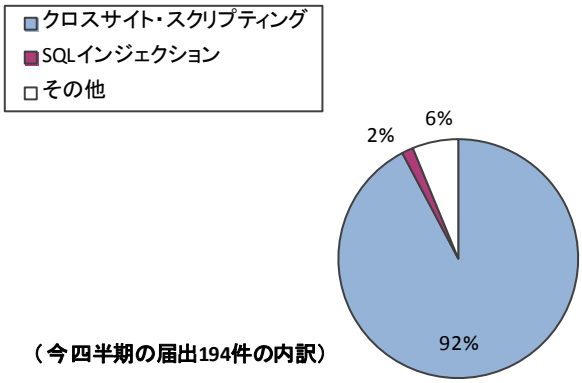


図5. 今四半期の脆弱性の種類の内訳

2.脆弱性の修正完了状況

～　ソフトウェア製品およびウェブサイトの修正件数が 4,100 件を突破しました　～

表 3 は 2011 年第 3 四半期のソフトウェア製品とウェブサイトの修正完了件数および届出開始から今四半期までの累計件数を示しています。

ソフトウェア製品の脆弱性の届出に関して、JPCERT/CC が調整を行い、製品開発者が修正を完了し、 2011 年第 3 四半期に JVN [*2] で対策情報を公表したものは 29 件（累計 545 件）でした。2010 年第 4 四半期以降は公表件数が 30 件前後で推移しています。JVN で公表した 29 件の脆弱性対策情報について、脆弱性の種類は「クロスサイト・スクリプティング」が 11 件と最も多く、次いで「サービス運用妨害」が 3 件などです（別紙 2 表 1-3 参照）。

表 3.　修正完了件数

分類	今期件数	累計件数
ソフトウェア製品	**29** 件	**545** 件
ウェブサイト	**86** 件	**3,596** 件
合計	**115** 件	**4,141** 件

今四半期に公表した 29 件のうち、届出を受理してから 45 日以内に公表した届出は 0 件でした。

IPA および JPCERT/CC は、製品開発者に速やかな対策および JVN で脆弱性対策情報を公表するための協力を期待します。

[*2] 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表し、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/

ウェブサイトの脆弱性関連情報の届出に関して、IPA がウェブサイト運営者に通知を行い、2011 年第 3 四半期に修正を完了したものは 86 件（累計 3,596 件）でした。修正完了した 86 件の内訳は、ウェブアプリケーションを修正したものが 73 件（85%）、当該ページを削除したものが 13 件（15%）でした。なお、修正完了した 86 件のうち 55 件（64%）は、届出から修正完了まで 1 年以上経過していました。**ウェブサイト運営者による、速やかな対策実施を期待します。**

3. 届出された脆弱性関連情報における連絡不能な製品開発者の一覧を公表

～製品開発者との調整が滞っている脆弱性関連情報の対策実施を促進～

IPA と JPCERT/CC は、2011 年 3 月に公開した「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- 2010 年版 -[*3]」にて定めた手続きに基づき、2011 年 9 月 29 日に連絡不能開発者 50 件を掲載した「連絡不能開発者一覧」を公表しました。

これにより、製品開発者および製品の関係者からの情報提供を求めていることの周知を図り、連絡が取れずに調整が滞っていた製品開発者に、届出されたソフトウェア製品の脆弱性対策の実施を促します。

今回の公表までの手続きにおいて、「連絡が取れない開発者名一覧の公表」の予告を伴った JPCERT/CC からの連絡により、これまで応答がなかった 18 の製品開発者から応答があり、調整に着手または調整の再開ができました。また、一覧の公表後すぐ、1 者と連絡が取れ、それらの調整に着手または調整を再開することができました。

IPA、JPCERT/CC は、今後もこの取り組みを進めるとともに、製品開発者に対しては、連絡不能とならないよう、脆弱性が発見された際の連絡先の明示および連絡体制の確立についての協力を期待します。

4. 脆弱性関連情報を届出する発見者の傾向

～届出する発見者が所属する組織の傾向が変化してきています～

2011 年になり、脆弱性関連情報を届け出た発見者が所属している組織の傾向が変化してきています。図 6 は、過去 3 年間の脆弱性関連情報を届け出た発見者が所属している組織の割合を示しています（発見者の自己申告情報から集計）。2009 年においては、所属している組織が「個人」74%、「企業」25%、「団体」1%、2010 年においては、「個人」50%、「企業」48%、「団体」1%、「教育・学術機関」1%であり、2009 年、2010 年においては、「企業」と「個人」による届出が 9 割以上を占めていました。

しかし、2011 年（9 月末時点）においては、所属している組織が個人 31%、企業 21%、「教育・学術機関」48%となっており、「教育・学術機関」である「大学院、大学」および「高等学校」、「専門学校」からの届出が半数を占めています。

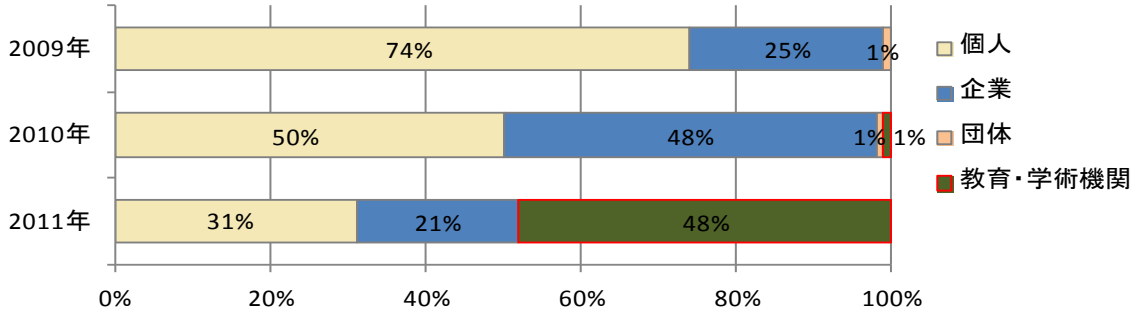


図6. 届出をした発見者が所属している組織の内訳

[*3] 「情報システム等の脆弱性情報の取扱いに関する研究会」2010 年度報告書
http://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html

本届出制度は、「情報セキュリティ早期警戒パートナーシップ」に賛同する関係者の協力のもと運営しており、これからもより広範な組織に対して本届出制度への理解・協力を得られるよう注力し、本届出制度の実効性を高め、より安心してソフトウェア製品、ウェブサイトを利用できる情報社会の確立に寄与していきます。

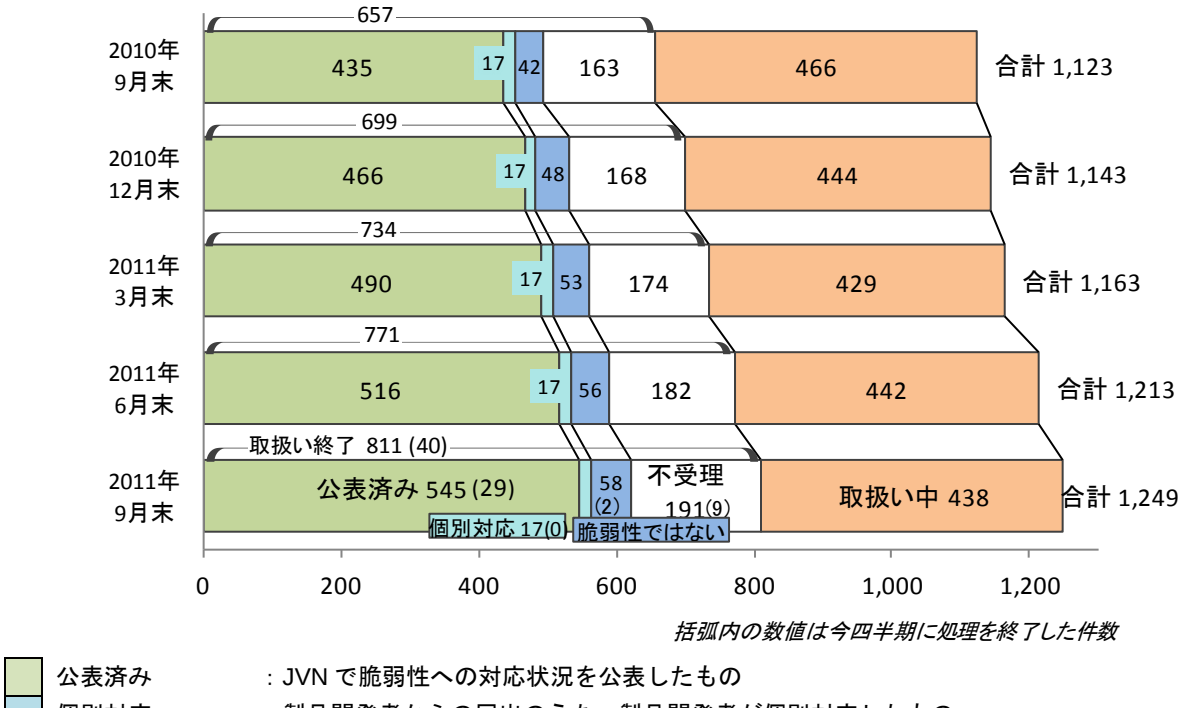
別紙 2

ソフトウェア等の脆弱性に関する届出の処理状況（詳細）

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

図 1-1 のグラフはソフトウェア製品の脆弱性関連情報の届出について、処理状況の推移を示したものです。今四半期に公表した脆弱性は 29 件（累計 545 件）です。また、製品開発者が「個別対応」したものは 0 件（累計 17 件）、製品開発者が「脆弱性ではない」と判断したものは 2 件（累計 58 件）、「不受理」としたものは 9 件 (*4)（累計 191 件）、取扱い中は 438 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 届出のあったソフトウェア製品の種類

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品に関する脆弱性関連情報 1,249 件のうち、不受理を除いた 1,058 件について、図 1-2 のグラフは製品種類別の届出件数の割合を、図 1-3 は過去 2 年間の製品種類別の届出件数の四半期別推移をそれぞれ示したものです。

今四半期における製品の種類は「その他」が多くなっています。これは、Android アプリが多く届出されたためです。

(*4) 今四半期の届出で不受理とした 1 件、前四半期までの届出の中で今四半期に不受理とした 8 件の合計です。

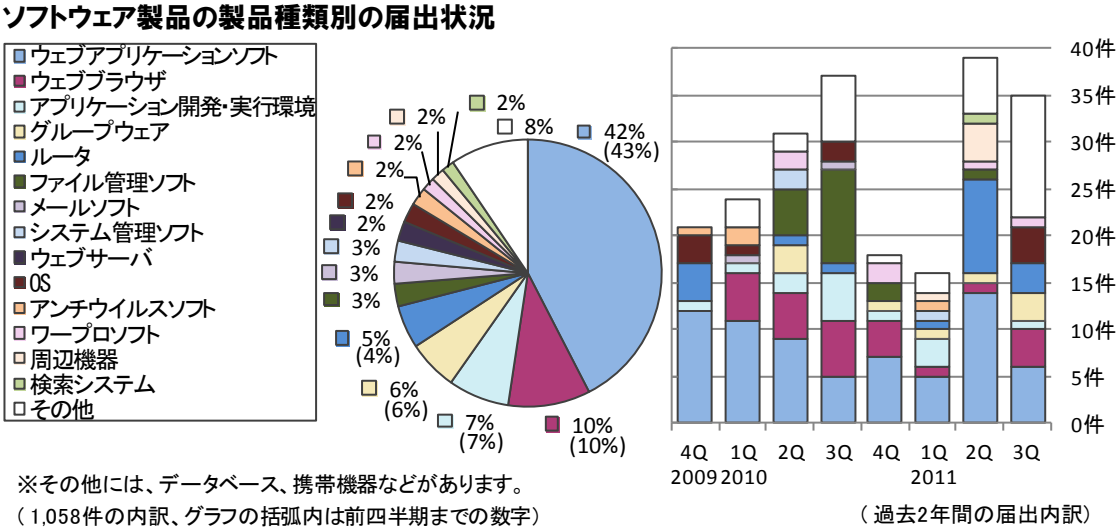


図1-2. 製品種類別の届出件数の割合

図1-3. 製品種類別の届出件数（四半期別推移）

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品に関する脆弱性関連情報 1,249 件のうち、不受理のものを除いた 1,058 件について、図 1-4 のグラフは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割合を、図 1-5 は過去 2 年間のオープンソースソフトウェアの届出件数の四半期別推移をそれぞれ示したものです。届出受付開始から今四半期までの届出のうち、オープンソースソフトウェアの届出は約 34%となっています。また、今四半期はオープンソースソフトウェアの届出が 7 件ありました。

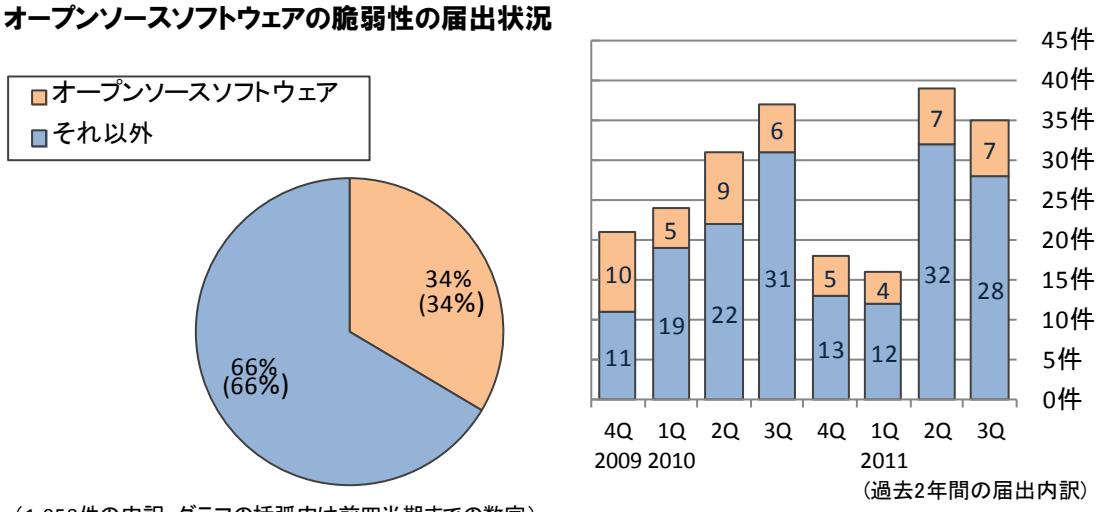


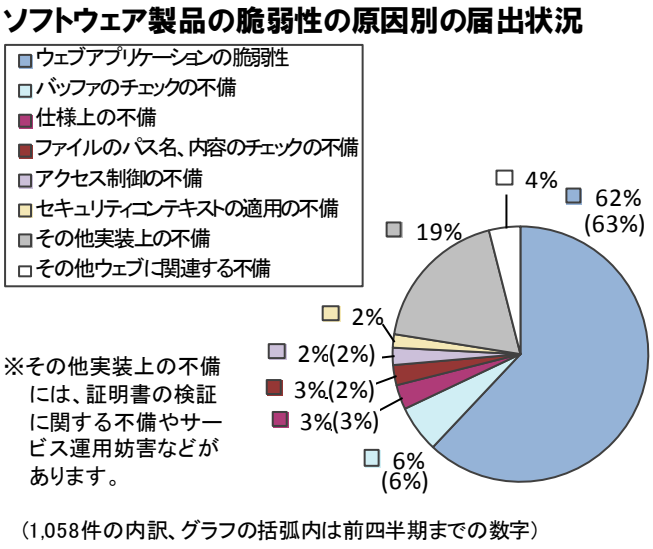
図1-4. オープンソースソフトウェアの届出件数の割合

図1-5. オープンソースソフトウェアの届出件数（四半期別推移）

1.3 脆弱性の原因と脅威

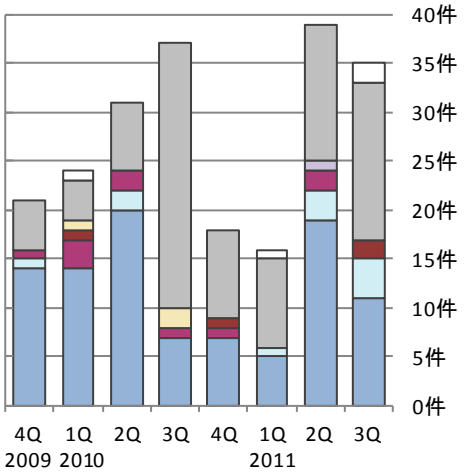
届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品に関する脆弱性関連情報 1,249 件のうち、不受理のものを除いた 1,058 件について、図 1-6 のグラフは原因別[*5]の届出件数の割合を、図 1-7 は過去 2 年間の原因別届出件数の四半期別推移をそれぞれ示したものです。ソフトウェア製品の脆弱性の原因は「ウェブアプリケーションの脆弱性」が最多となっています。この傾向は受付開始から 2010 年第 2 四半期まで継続していましたが、2010 年第 3 四半期から「その他実装上の不備」の割合が増加し、今四半期では最多となっています。

[*5] それぞれの詳しい脆弱性の原因の説明については付表 1 を参照してください。



（1,058件の内訳、グラフの括弧内は前四半期までの数字）

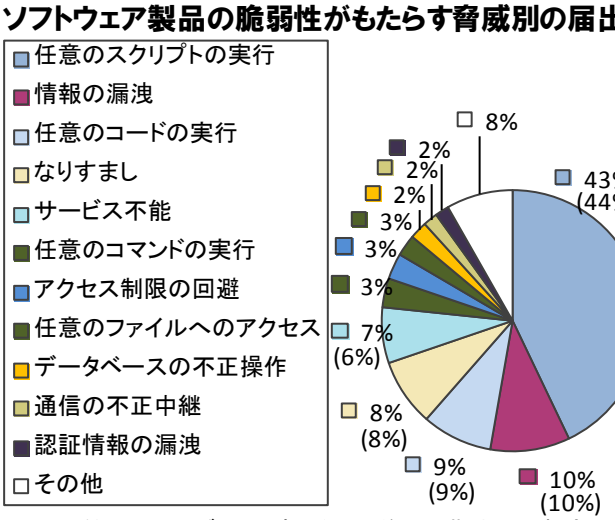
図1-6. 脆弱性の原因別の届出件数の割合



（過去2年間の届出内訳）

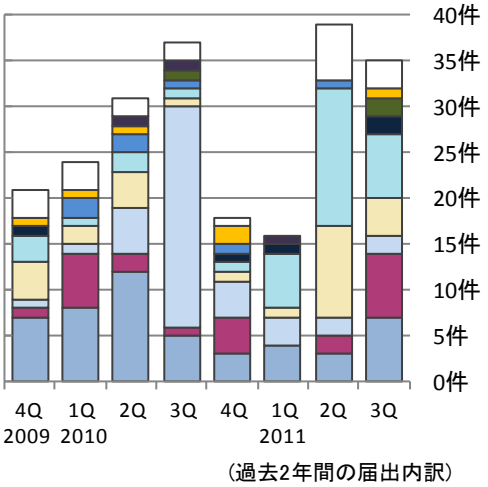
図1-7. 脆弱性の原因別の届出件数（四半期別推移）

図 1-8 のグラフは脆弱性がもたらす脅威別の届出件数の割合を、図 1-9 は過去 2 年間の脆弱性がもたらす脅威別届出件数の四半期別推移をそれぞれ示したものです。脆弱性がもたらす脅威は「任意のスクリプト実行」が半数近くを占めています。また、2011 年第 1 四半期から「サービス不能」が増加傾向にあります。



（1,058件の内訳、グラフの括弧内は前四半期までの数字）

図1-8. 脆弱性がもたらす脅威別の届出件数の割合



（過去2年間の届出内訳）

図1-9. 脆弱性がもたらす脅威別の届出件数（四半期別推移）

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

表 1-1 は今四半期の脆弱性の公表件数および届出開始から今四半期までの累計公表件数を示しています。JPCERT/CC は、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や関係者との調整、および海外 CSIRT 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[*6]。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）（URL： http://jvn.jp/ ）において公表しています。図 1-10 のグラフは、届出受付開始から今四半期までの届出の中で、対策情報を公表した 1,224 件について、過去 3 年間の公表件数の四半期別推移を示したものです。

[*6] JPCERT/CC 活動概要 Page18~24（https://www.jpcert.or.jp/pr/2011/PR20111011.pdf）を参照下さい。

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	今期件数	累計件数
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、対策方法について届出を受けたもの	29 件	545 件
②	海外 CSIRT 等と連携して公表したもの	26 件	679 件
	合計	55 件	1,224 件

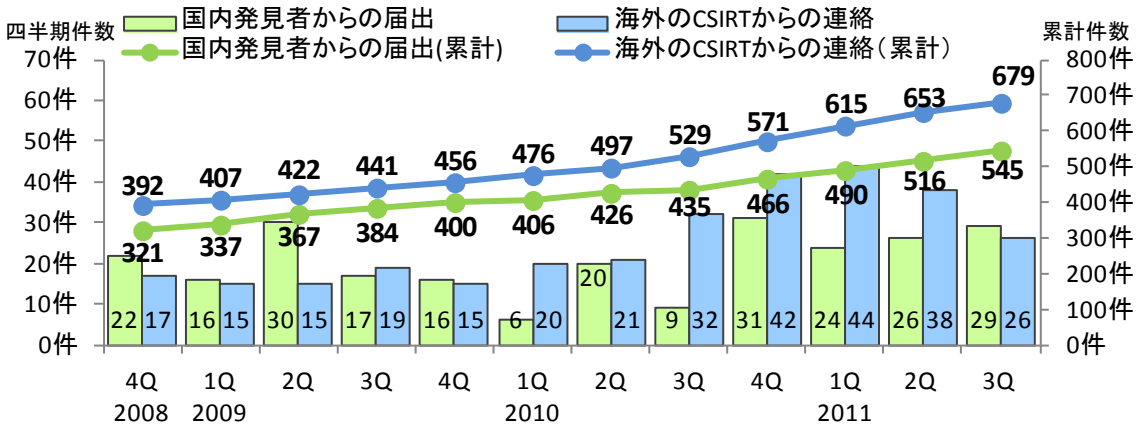


図1−10. ソフトウェア製品の脆弱性対策情報の公表件数

（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

届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性関連情報（表 1-1 の①）について、図 1-11 は受理してから JVN 公表するまでに要した日数を示したものです。表 1-2 は過去 3 年間における 45 日以内に公表した件数の割合推移を四半期別に示したものです。45 日以内に公表した件数は 2011 年第 3 四半期で 34%、45 日を超過した件数は 66%です。2011 年第 2 四半期に引き続き割合が減少していますが、これは、2011 年第 3 四半期に 45 日以上超過した届出を多く公表したためです。製品開発者は脆弱性を攻撃された場合の危険性を認識し、迅速な対策を講じる必要があります。

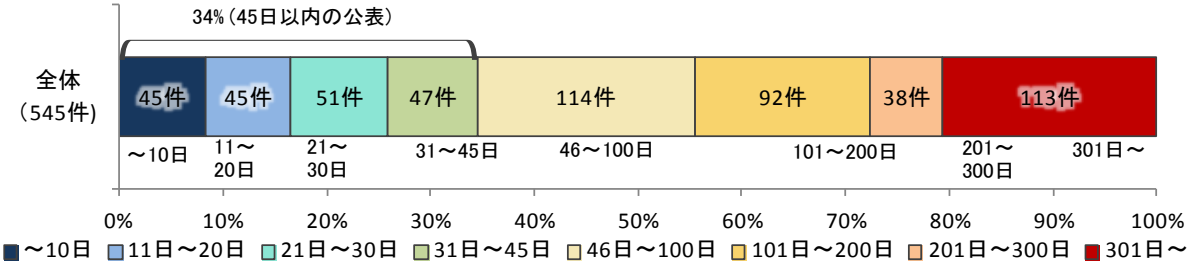


図1−11. ソフトウェア製品の脆弱性公表日数

表 1-2.　45 日以内の公表件数の四半期別推移

2008 4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q
34%	33%	34%	35%	35%	35%	36%	36%	38%	38%	36%	34%

表 1-3 は国内の発見者および製品開発者から届出があり、今四半期に JVN 公表した脆弱性を示しています。オープンソースソフトウェアに関し公表したものが 18 件（表 1-3 の*1）、組込みソフトウェア製品の脆弱性が 2 件（表 1-3 の*2）ありました。

表 1-3. 2011 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	「Opera」におけるサービス運用妨害 (DoS) の脆弱性	ウェブブラウザ「Opera」には、サービス運用妨害 (DoS) の脆弱性がありました。このため、細工されたウェブページにアクセスすると、ハードディスクの空き容量が枯渇させられる可能性がありました。	2011 年 7 月 5 日	4.3
2	「XnView」における実行ファイル読み込みに関する脆弱性	画像管理ソフトウェア「XnView」には、実行ファイルを読み込む際のファイル検索パスに問題があり、意図しない実行ファイルを読み込んでしまう脆弱性が存在しました。このため、第三者によりプログラムを実行している権限で任意のコードを実行される可能性がありました。	2011 年 7 月 5 日	5.1
3 (*2)	「Google 検索アプライアンス」におけるクロスサイト・スクリプティングの脆弱性	検索システム「Google 検索アプライアンス」には、UTF-7 で記述された特定の文字列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る可能性がありました。	2011 年 7 月 15 日	4.3
4	「ASP.NET」におけるクロスサイト・スクリプティングの脆弱性	Web アプリケーションフレームワーク「ASP.NET」には、クロスサイト・スクリプティングの脆弱性が存在するモバイル端末向けウェブアプリケーションを作り出す問題がありました。このため、「ASP.NET」を用いたウェブアプリケーションに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。	2011 年 7 月 15 日	4.3
5	「Oracle iPlanet Web Server」における情報漏えいの脆弱性	ウェブサーバ「Oracle iPlanet Web Server」（旧名：「Sun Java System Web Server」）には、情報漏えいの脆弱性がありました。このため、「Oracle iPlanet Web Server」で動作するウェブアプリケーションのソースコードが漏えいする可能性がありました。	2011 年 7 月 25 日	5.0
6 (*1)	「Android」における SSL 証明書の表示に関する脆弱性	「Android」には、外部サイトの SSL 証明書を表示してしまう脆弱性がありました。このため、安全なサイトにアクセスしていると誤認してしまい、フィッシング詐欺などの被害を受ける可能性がありました。	2011 年 7 月 29 日	4.3
7	「Windows」の URL プロトコルハンドラにおける実行ファイル読み込みに関する脆弱性	「Windows」の URL プロトコルハンドラには、実行ファイルを読み込む際のファイル探索パスに問題があり、意図しない実行ファイルを読み込んでしまう脆弱性が存在しました。このため、第三者により任意のコードを実行される可能性がありました。	2011 年 8 月 10 日	6.8
8	「Internet Explorer」におけるウィンドウ偽装の脆弱性	ウェブブラウザ「Internet Explorer」には、ウィンドウの表示を偽装することが可能な脆弱性が存在しました。このため、ウィンドウ内のアドレスバーを偽装することで、フィッシング詐欺などに使用される可能性がありました。	2011 年 8 月 12 日	4.3
9 (*1)	「Aipo」における SQL インジェクションの脆弱性	グループウェア「Aipo」には、利用者から入力された内容を元に SQL 文を組み立てる処理に問題がありました。このため、Aipo にログイン可能な第三者により任意の SQL 命令を実行される可能性がありました。	2011 年 8 月 16 日	6.5

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
10	「Windows XP」におけるサービス運用妨害 (DoS) の脆弱性	「Windows XP」には、サービス運用妨害 (DoS) の脆弱性がありました。このため、第三者により細工されたパケットを送付されることで、サービス運用妨害 (DoS) 状態にされる可能性がありました。	2011 年 8 月 19 日	4.3
11 (*1)	「WebsiteBaker」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「WebsiteBaker」には、出力する文字列のエスケープ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スクリプトを埋め込まれる可能性がありました。	2011 年 8 月 26 日	4.3
12 (*1)	「Samba Web Administration Tool」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	Samba 管理ツール「Samba Web Administration Tool」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、Samba の設定を変更される可能性がありました。	2011 年 8 月 26 日	4.0
13 (*1)	「Sage」において任意のスクリプトが実行される脆弱性	RSS リーダ「Sage」には、フィード内の情報を HTML ページに出力する際のエスケープ処理に問題がありました。14 で修正された問題とは異なります。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。	2011 年 9 月 2 日	5.8
14 (*1)	「Sage」において任意のスクリプトが実行される脆弱性	RSS リーダ「Sage」には、フィード内の情報を HTML ページに出力する際のエスケープ処理に問題がありました。13 で修正された問題とは異なります。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。	2011 年 9 月 2 日	5.8
15 (*2)	「Juniper Networks IDP ACM」におけるクロスサイト・スクリプティングの脆弱性	Juniper 製品管理ツール「IDP ACM」には、出力する文字列のエスケープ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スクリプトを埋め込まれる可能性がありました。	2011 年 9 月 2 日	4.3
16 (*1)	「GTK+」における DLL 読み込みに関する脆弱性	GUI アプリケーションの作成ソフト「GTK+」には、DLL を読み込む際の DLL 検索パスに問題があり、意図しない DLL を読み込んでしまう脆弱性が存在しました。このため、第三者によりプログラムを実行している権限で任意のコードを実行される可能性がありました。	2011 年 9 月 2 日	6.8
17	「Megalith」における認証回避の脆弱性	掲示板ソフトウェア「Megalith」には、認証回避が可能な脆弱性がありました。このため、第三者により管理者権限を奪取される可能性がありました。	2011 年 9 月 9 日	6.4
18 (*1)	「BaserCMS」 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「BaserCMS」には、出力する文字列のエスケープ処理に問題がありました。このため、ユーザのウェブブラウザ上で任意のスクリプトを実行される可能性がありました。	2011 年 9 月 30 日	4.3
19 (*1)	「BaserCMS」 におけるアクセス制限不備の脆弱性	コンテンツ管理システム「BaserCMS」には、アクセス制限不備の脆弱性が存在しました。このため、「BaserCMS」にログイン可能な第三者により、管理者のユーザ情報が変更されるなどの可能性がありました。	2011 年 9 月 30 日	4.9
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
20	「Internet Explorer」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ「Internet Explorer」には、EUC-JP で記述された特定の文字列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る可能性がありました。	2011 年 7 月 8 日	2.6

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
21 (*1)	「Plone」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「Plone」には、出力する文字列のエスケープ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スクリプトを埋め込まれる可能性がありました。	2011 年 7 月 27 日	2.6
22 (*1)	「Mozilla Firefox」における Content-Length ヘッダの処理に関する脆弱性	ウェブブラウザ「Mozilla Firefox」には、HTTP レスポンスに含まれる Content-Length ヘッダの処理に関する脆弱性がありました。このため、他ドメインのレスポンス中にスクリプトを混入される可能性がありました。	2011 年 7 月 28 日	2.6
23 (*1)	「Mozilla Firefox」におけるサービス運用妨害 (DoS) の脆弱性	ウェブブラウザ「Mozilla Firefox」にはサービス運用妨害 (DoS) の脆弱性がありました。このため、細工された認証局の証明書を取り込んだ状態で HTTPS 接続すると、サービス運用妨害 (DoS) 状態にされる可能性がありました。	2011 年 7 月 28 日	2.6
24 (*1)	「Mozilla Firefox」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ「Mozilla Firefox」には、特定の数値文字参照の解釈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る可能性がありました。	2011 年 7 月 28 日	2.6
25 (*1)	「Mozilla Firefox」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ「Mozilla Firefox」には、スタイルシート (CSS) の解釈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る可能性がありました。	2011 年 7 月 28 日	2.6
26 (*1)	「Aipo」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「Aipo」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、管理者が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、当該製品で管理している情報を改ざんされる可能性がありました。	2011 年 8 月 16 日	2.6
27 (*1)	「Samba Web Administration Tool」におけるクロスサイト・スクリプティングの脆弱性	Samba 管理ツール「Samba Web Administration Tool」には、出力する文字列のエスケープ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スクリプトを埋め込まれる可能性がありました。	2011 年 8 月 26 日	2.6
28 (*1)	「Phorum」における複数の脆弱性	掲示板ソフトウェア「Phorum」には、クロスサイト・リクエスト・フォージェリとクロスサイト・スクリプティングの脆弱性がありました。このため、ログインしているユーザの意図に反してファイルがアップロードされたり、ウェブブラウザ上で任意のスクリプトが実行されたりする可能性がありました。	2011 年 9 月 2 日	2.6
29 (*1)	「SemanticScuttle」におけるクロスサイト・スクリプティングの脆弱性	ブックマーク管理ソフトウェア「SemanticScuttle」には、出力する文字列のエスケープ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スクリプトを埋め込まれる可能性がありました。	2011 年 9 月 16 日	2.6

（*1）：オープンソースソフトウェア製品の脆弱性
（*2）：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

表 1-4、表 1-5 は JPCERT/CC が海外 CSIRT 等と連携し、今四半期に公表した脆弱性および対応状況を示しています。今四半期に公表した脆弱性は 29 件あり、うち表 1-4 には通常の脆弱性情報 21 件、表 1-5 には対応に緊急を要する Technical Cyber Security Alert の 5 件を示しています。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 1-4.米国 CERT/CC (*7) 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	ISC BIND にサービス運用妨害 (DoS) の脆弱性	緊急案件として掲載 複数製品開発者へ通知
2	ISC BIND 9.8 系にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 複数製品開発者へ通知
3	libpng における sCAL チャンクの処理に脆弱性	特定製品開発者へ通知
4	Brocade BigIron RX スイッチにアクセス制御リスト (ACL) 回避の脆弱性	注意喚起として掲載
5	ArcSight Connector Appliance 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
6	Apple iOS における複数の脆弱性に対するアップデート	注意喚起として掲載
7	Oracle Outside In に任意のコードが実行される脆弱性	注意喚起として掲載
8	Apple Safari における複数の脆弱性に対するアップデート	注意喚起として掲載
9	Apple iOS における脆弱性に対するアップデート	注意喚起として掲載
10	Secure Access Link (SAL) Gateway に情報漏えいの脆弱性	注意喚起として掲載
11	Apple Quicktime における複数の脆弱性に対するアップデート	注意喚起として掲載
12	RT-N56U における管理パスワード漏えいの脆弱性	注意喚起として掲載
13	Apache HTTPD サーバにサービス運用妨害 (DoS) の脆弱性	緊急案件として掲載 複数製品開発者へ通知
14	LifeSize Room に複数の脆弱性	注意喚起として掲載
15	Apple Mac OS X におけるアップデート	注意喚起として掲載
16	Mercator SENTINEL に SQL インジェクションの脆弱性	注意喚起として掲載
17	JasperServer にクロスサイトリクエストフォージェリの脆弱性	注意喚起として掲載
18	AmmSoft ScriptFTP 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
19	libpng における cHRM チャンクの処理に脆弱性	注意喚起として掲載
20	Quagga に複数の脆弱性	特定製品開発者へ通知
21	SSL と TLS の CBC モードに選択平文攻撃の脆弱性	注意喚起として掲載

表 1-5.米国 US-CERT (*8) 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に対するアップデート
2	Oracle 製品における複数の脆弱性に対するアップデート
3	Microsoft 製品における複数の脆弱性に対するアップデート
4	Adobe 製品における複数の脆弱性
5	Microsoft 製品における複数の脆弱性に対するアップデート

(*7) 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。

(*8) United States Computer Emergency Readiness Team：米国の政府系 CSIRT。

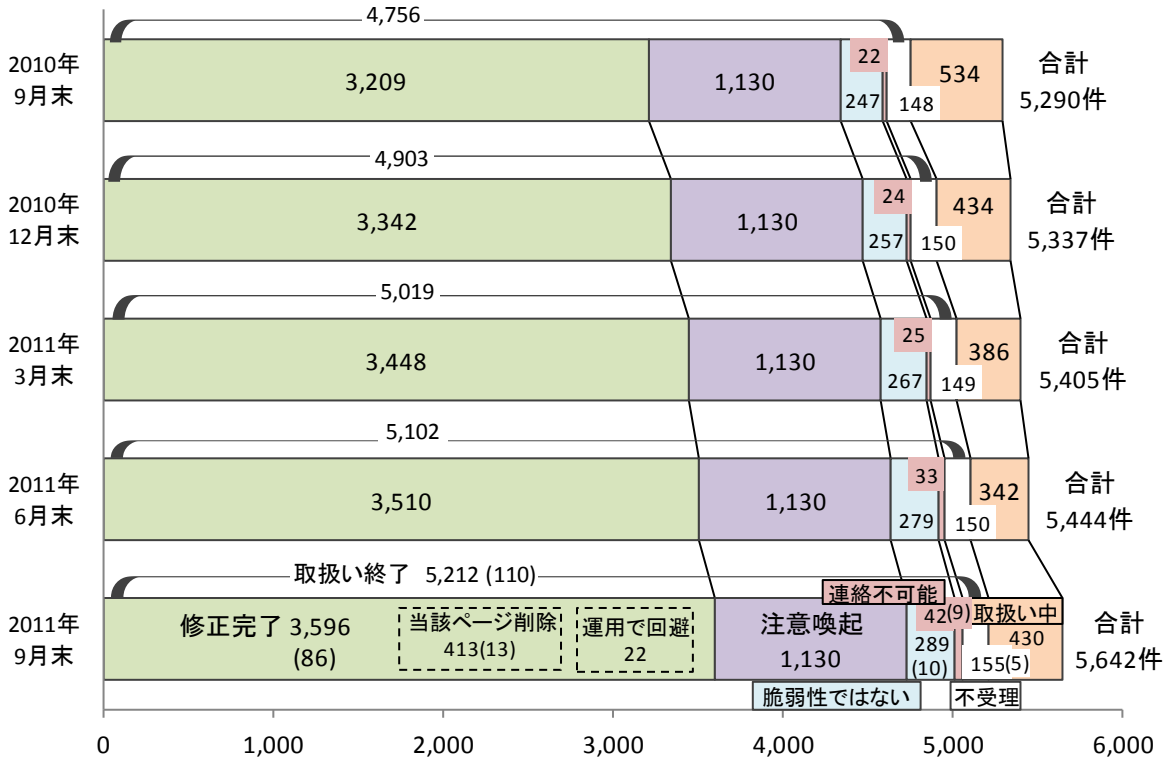
2. ウェブサイトの脆弱性の処理状況の詳細

2.1 ウェブサイトの脆弱性の処理状況

図 2-1 はウェブサイトの脆弱性関連情報の届出について、処理状況の推移を示したものです。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 110 件（累計 5,212 件）でした。このうち「修正完了」したものは 86 件（累計 3,596 件）、ウェブサイトが利用しているソフトウェア製品の修正プログラムが適用されていない問題について、IPA による「注意喚起」で広く対策実施を促したあと処理を取りやめたものは 0 件（累計 1,130 件）、IPA および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 10 件（累計 289 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るなどの対応をしていますが、それでもウェブサイト運営者と連絡が取れず「連絡不可能」なものは 9 件（累計 42 件）です。「不受理」としたものは 5 [*9] 件（累計 155 件）でした。

取扱いを終了した累計 5,212 件のうち「注意喚起」「連絡不可能」「不受理」を除く累計 3,885 件（75%）は、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されたことを確認しました。

「修正完了」したもののうち、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 13 件（累計 413 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 22 件）でした。



①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
該当ページを削除	：	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
②注意喚起	：	IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
③脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
④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
⑤不受理	：	告示で定める届出の対象に該当しないもの
⑥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

[*9] 今四半期の届出で不受理とした 4 件、前四半期までの届出の中で今四半期に不受理とした 1 件の合計です。

2.2 ウェブサイトの運営主体の種類

図 2-2 のグラフは過去 2 年間に IPA に届出のあったウェブサイトの脆弱性関連情報のうち、不受理のものを除いたウェブサイトの運営主体の種類別届出件数の四半期別推移を示しています。今四半期も企業が多くありました。

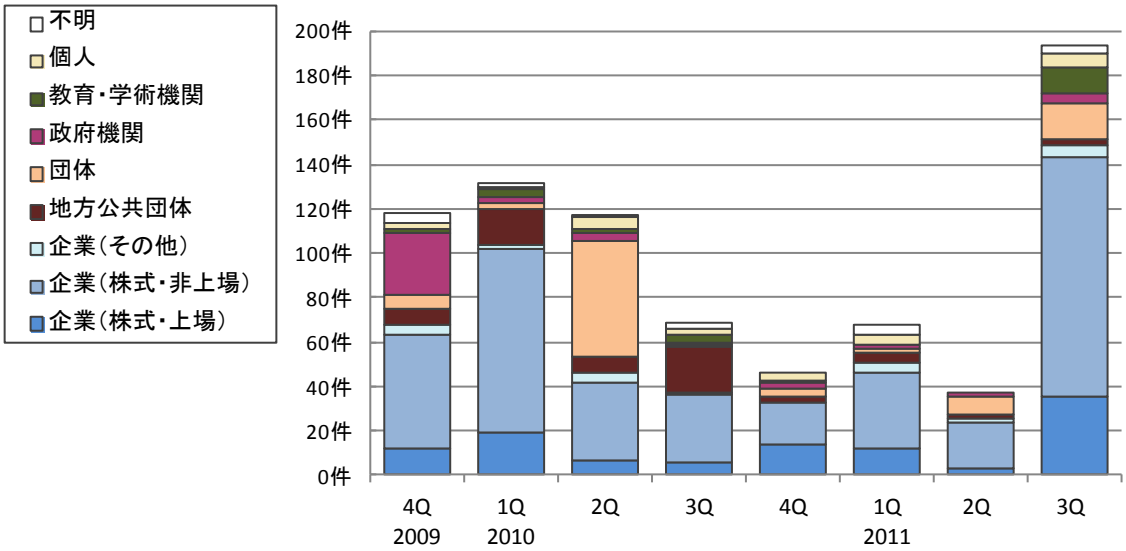
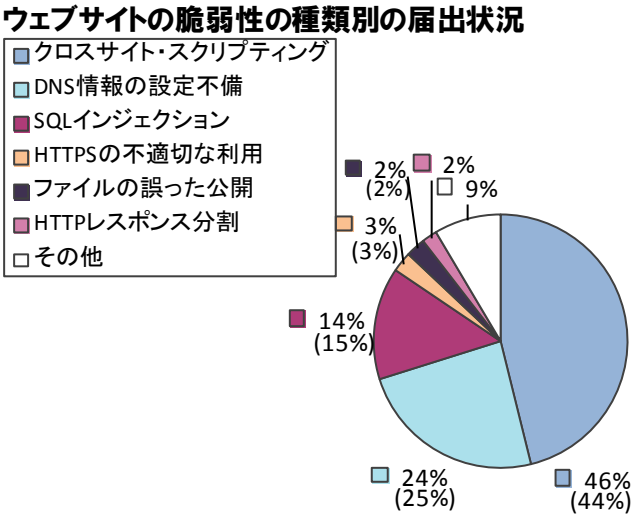


図2-2. ウェブサイトの運営主体の種類別の届出件数（四半期別推移）

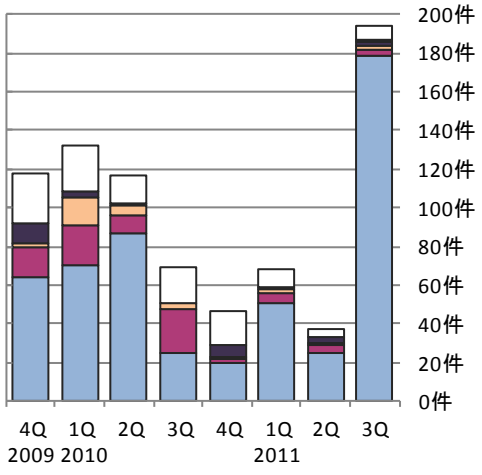
2.3 ウェブサイトの脆弱性の種類と脅威

届出受付開始から今四半期までに IPA に届出のあったウェブサイトの脆弱性関連情報 5,642 件のうち、不受理のものを除いた 5,487 件について、図 2-3 のグラフは脆弱性の種類別の届出件数の割合を、図 2-4 は過去 2 年間の脆弱性の種類別届出件数の四半期別推移をそれぞれ示したものです[*10]。脆弱性の種類は届出の多い「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」にて全体の 84%を占めています。2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS 情報の設定不備」は、2009 年第 4 四半期以降は届出がありません。今四半期の届出（194 件）のうち、「クロスサイト・スクリプティング」だけで 92%（179 件）を占めます。



（5,487件の内訳、グラフの括弧内は前四半期までの数字）

図2-3. 脆弱性の種類別の届出件数の割合

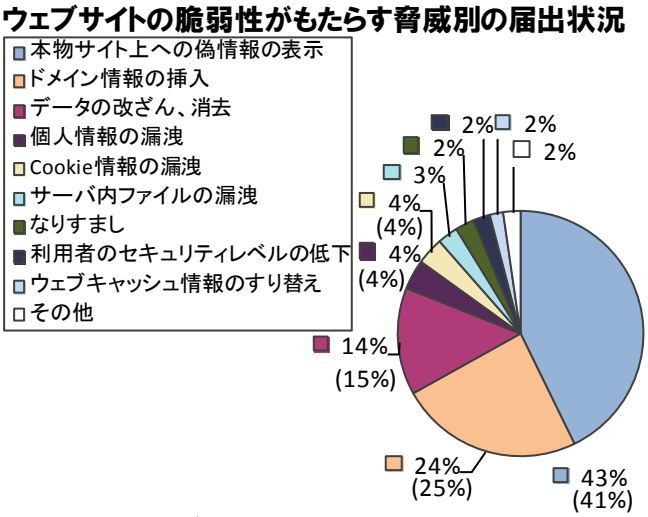


（過去2年間の届出内訳）

図2-4. 脆弱性の種類別の届出件数（四半期別推移）

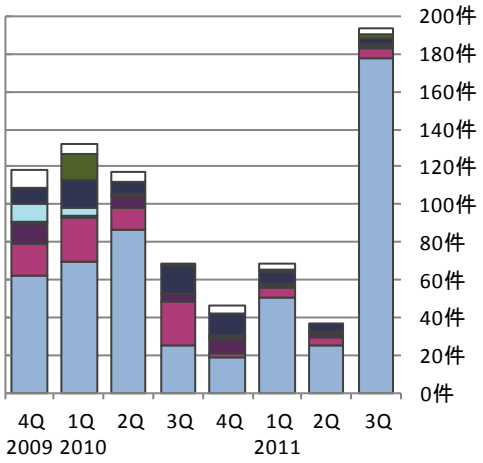
[*10] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

図 2-5 のグラフは脆弱性がもたらす脅威別の届出件数の割合を、図 2-6 は過去 2 年間の脆弱性がもたらす脅威別届出件数の四半期別推移をそれぞれ示したものです。脆弱性がもたらす脅威は「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」にて全体の 81%を占めています。



(5,487件の内訳、グラフの括弧内は前四半期までの数字)

図2-5. 脆弱性がもたらす脅威別の届出件数の割合



(過去2年間の届出内訳)

図2-6. 脆弱性がもたらす脅威別の届出件数(四半期別推移)

2.4 ウェブサイトの脆弱性の修正完了状況

図 2-7 のグラフは、ウェブサイトの脆弱性について過去 3 年間の四半期別の修正完了件数を示しています。表 2-1 は、過去 3 年間の四半期末の時点で、修正が完了した全届出のうち、ウェブサイト運営者に脆弱性関連情報を通知してから、90 日以内に修正が完了した件数の割合を示したものです。2009 年第 3 四半期以降は、301 日以上経過してから修正が完了した件数が増加しています。これは、取扱いが長期化しているものについて、IPA が脆弱性対策の実施を促す連絡を繰り返し実施したためです。

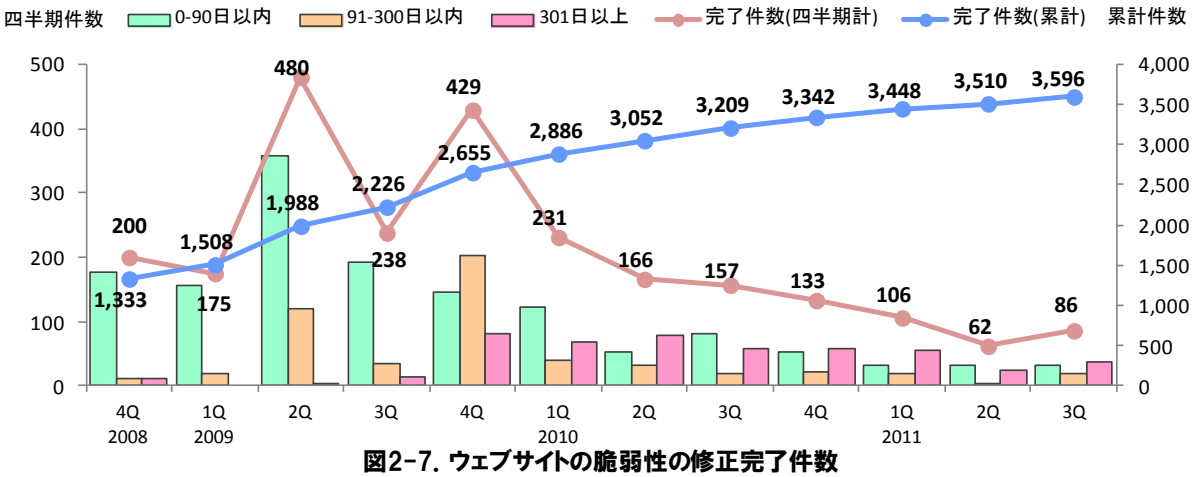


図2-7. ウェブサイトの脆弱性の修正完了件数

表 2-1. 90 日以内に修正完了した件数および割合の推移

	2008 4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q
修正完了件数	1,333	1,508	1,988	2,226	2,655	2,886	3,052	3,209	3,342	3,448	3,510	3,596
90 日以内の件数	1,057	1,212	1,569	1,760	1,905	2,028	2,082	2,163	2,216	2,247	2,280	2,311
90 日以内の割合	83%	80%	79%	79%	72%	70%	68%	67%	66%	65%	65%	64%

図 2-8 および図 2-9 は、ウェブサイト運営者に脆弱性関連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示したものです[*11]。全体の 46%の届出が 30 日以内、全体の 64%の届出が 90 日以内に修正されています。

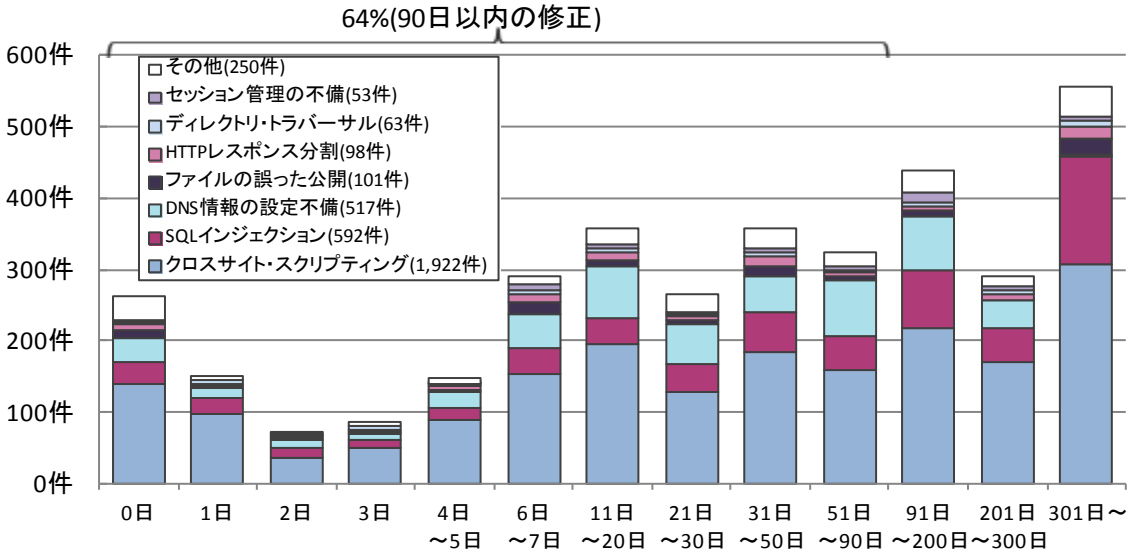


図2-8.ウェブサイトの修正に要した日数

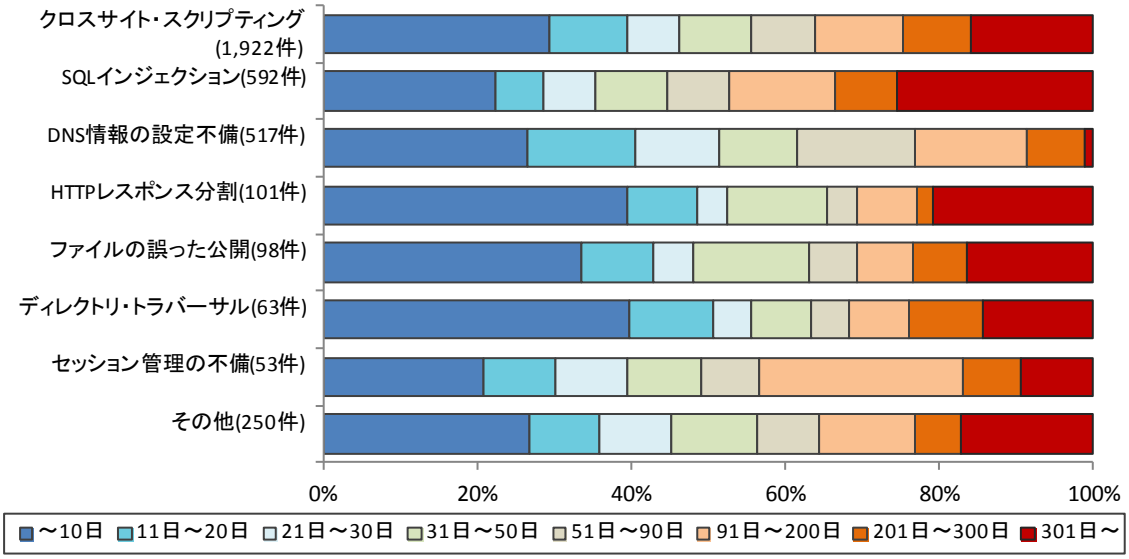


図2-9.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*11] 運営者から修正完了の報告があったもの、および、脆弱性が修正されたと IPA で判断したものも含めて示しています。なお、0 日は詳細情報を通知した当日に修正されたもの、または運営者へ詳細情報を通知する前に修正されたものです。

2.5 ウェブサイトの脆弱性の取扱中の状況

ウェブサイト運営者から脆弱性を修正した旨の通知が無い場合、IPA は脆弱性が攻撃された場合の危険性を分かりやすく解説することや、1～2 か月毎に電子メールや電話、郵送などの手段で脆弱性対策の実施を促しています。

図 2-10 は、ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから今四半期末までに脆弱性を修正した旨の通知が無く 90 日以上経過）しているものについて、経過日数別の件数を示したものです。経過日数が 90 日から 199 日に達したものは 13 件、200 日から 299 日のものは 13 件など、これらの合計は 228 件（前四半期は 289 件）です。前四半期末までの取扱い長期化 289 件のうち今四半期に 70 件が取扱い終了となった一方、新たに 9 件が 90 日以上経過し取扱い長期化に加わり、合計で前四半期から取扱い長期化の件数が 61 件減少しました。

表 2-2 は、過去 2 年間の四半期末時点で取扱い中の届出について、取扱いが長期化している届出件数および、長期化している割合の四半期別推移を示しています。2009 年第 3 四半期以降、取扱い中件数および長期化している件数が減少していましたが、今四半期は、取扱い中件数が増加しています。これは、届出件数が急増したことにより新規に取扱い中の件数が増加したためです。

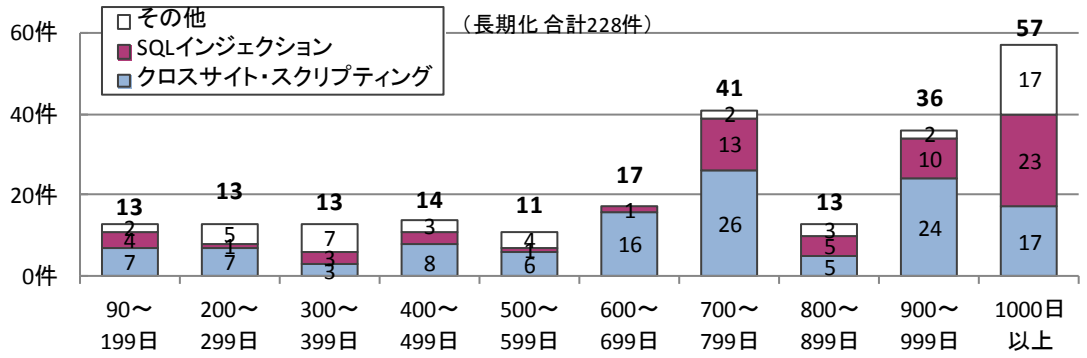


図2-10.取扱いが長期化（90日以上経過）しているウェブサイトの経過日数と脆弱性の種類

表 2-2. 取扱いが長期化している届出件数および割合の四半期別推移

	2009 4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q
取扱い中件数	819 件	707 件	651 件	534 件	434 件	386 件	342 件	430 件
長期化している件数	551 件	507 件	440 件	394 件	359 件	309 件	289 件	228 件
長期化している割合	67%	71%	68%	74%	83%	80%	85%	53%

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、迅速な対策を講じる必要があります。**

3. 関係者への要望

脆弱性の修正促進のための、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で利用している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/

また、対策実施にあたっては、以下のコンテンツが利用できます。

「安全なウェブサイトの作り方」: http://www.ipa.go.jp/security/vuln/websecurity.html

「安全な SQL の呼び出し方」: http://www.ipa.go.jp/security/vuln/websecurity.html

「Web Application Firewall 読本」: http://www.ipa.go.jp/security/vuln/waf.html

（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」へ登録ください（URL：https://www.jpcert.or.jp/vh/regist.html）。また、製品開発者自身が自社製品に関する脆弱性関連情報を発見した場合も、対策情報を利用者へ周知するために JVN を活用できます。JPCERT/CC もしくは IPA へ連絡してください。

なお、製品開発にあたっては、以下のコンテンツが利用できます。

「TCP/IP に係る既知の脆弱性検証ツール」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

「TCP/IP に係る既知の脆弱性に関する調査報告書」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」:
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

（3）一般インターネットユーザー

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る必要があります。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。

なお、MyJVN（URL：http://jvndb.jvn.jp/apis/myjvn/）では脆弱性対策情報を効率的に収集し、利用者の PC 上にインストールされたソフトウェア製品のバージョンを容易にチェックする等の機能を提供しています。

（4）発見者

脆弱性関連情報の適切な流通のため、届出し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、適切に管理してください。

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	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

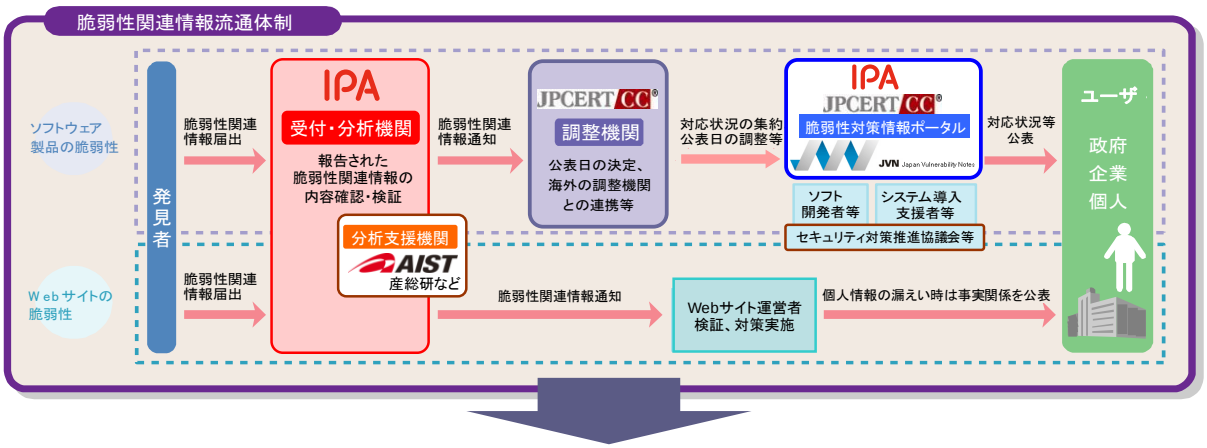
付表 2. ウェブサイト脆弱性の分類

	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個人情報等需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：一般社団法人 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