Information-technology Promotion Agency, Japan

JPCERT CC®

プレスリリース
2012 年 1 月 26 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 4 四半期（10 月～12 月）]

～スマートフォンに関連した脆弱（ぜいじゃく）性関連情報の届出が増加傾向～

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 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。

（1）脆弱性の届出件数の累計が 7,310 件に（別紙 1　1.参照）

2011 年第 4 四半期の IPA への脆弱性関連情報の届出件数は 427 件です。内訳は、ソフトウェア製品に関するものが 46 件、ウェブサイト（ウェブアプリケーション）に関するものが 381 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 1,285 件、ウェブサイトに関するものが 6,025 件、合計 7,310 件となりました。

（2）脆弱性の修正完了件数の累計が 4,400 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 4 四半期に JVN (*2) で対策情報を公表したものは 35 件（累計 580 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 4 四半期に修正を完了したものは 259 件（累計 3,855 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 4,435 件となりました。

（3）スマートフォンに関する脆弱性関連情報の届出が増加傾向（別紙 1　3.参照）

スマートフォンの普及に伴い、スマートフォン関連のソフトウェア製品（OS、アプリケーション）についての届出が増加傾向にあります。2011 年第 1 四半期および第 2 四半期においては届出全体の 10%未満でしたが、第 3 四半期には 29%、第 4 四半期には 38%に達しています。

スマートフォン関連のソフトウェア製品、特にアプリケーションの開発者には、脆弱性が発見された際の速やかな対応を期待します。

■ 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。

(*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/

別紙 1

2011 年第 4 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 7,310 件になりました ～

表 1 は 2011 年第 4 四半期の IPA への脆弱性関連情報の届出件数および届出受付開始（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 46 件、ウェブサイト（ウェブアプリケーション）に関するもの 381 件、合計 427 件でした。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 1,285 件、ウェブサイトに関するもの 6,025 件、合計 7,310 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。

表 1.　届出件数

分類	今期件数	累計件数
ソフトウェア製品	**46** 件	**1,285** 件
ウェブサイト	**381** 件	**6,025** 件
合計	**427** 件	**7,310** 件

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微増となり、ウェブサイトの届出は前四半期の約 2 倍となっています。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 4 四半期末で 4.01 (*1) 件となりました。

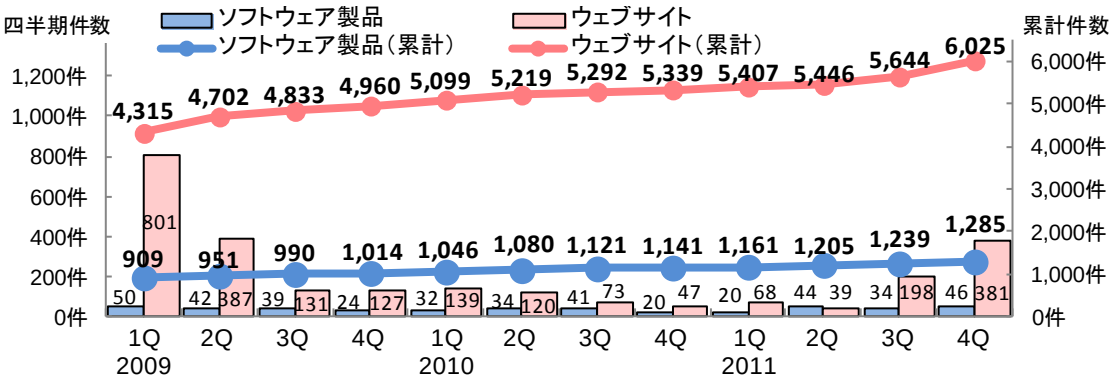


図 1.脆弱性関連情報の届出件数の四半期別推移

表 2. 届出件数（過去 3 年間）

	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q
累計届出件数[件]	5,224	5,653	5,823	5,974	6,145	6,299	6,413	6,480	6,568	6,651	6,883	7.310
1就業日あたり[件/日]	4.53	4.65	4.56	4.47	4.40	4.32	4.22	4.10	4.00	3.91	3.90	4.01

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 46 件のうち、不受理を除いた 45 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「ウェブブラウザ」が最も多く、次いで「ウェブアプリケーションソフト (*2) 」と「ルータ」となっています。脆弱性がもたらす脅威は「任意のファイルへのアクセス」、「任意のスクリプトの実行」、「情報の漏洩」が多く届出されており、これらの届出で全体の 64%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
(*2)　製品として提供されているソフトウェア（ウェブサーバ、ウェブアプリケーションサーバ等）

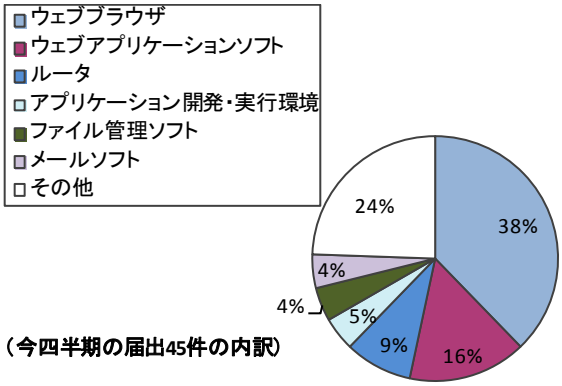


図2. 今四半期のソフトウェア製品種類の内訳

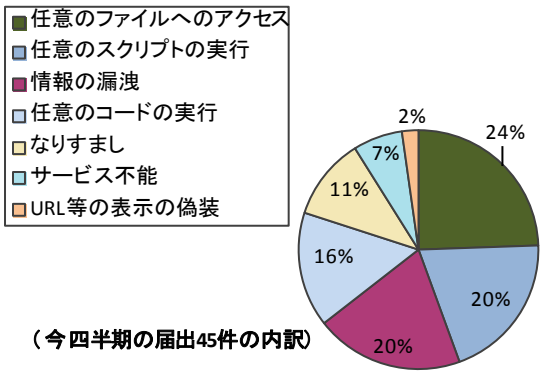


図3. 今四半期の脆弱性がもたらす脅威の内訳

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 381 件のうち、不受理を除いた 379 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 78%を占めています。また、脆弱性の種類は前四半期と同様に「クロスサイト・スクリプティング」が最も多く、全体の 96%を占めています。

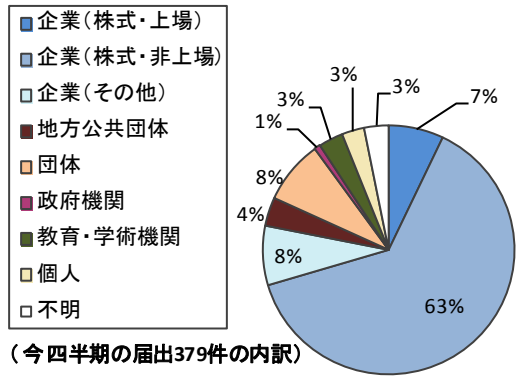


図4. 今四半期のウェブサイト運営主体の内訳

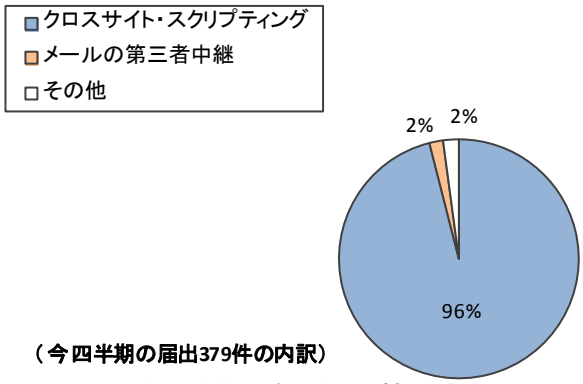


図5. 今四半期の脆弱性の種類の内訳

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 4,400 件を突破しました　～

表 3 は 2011 年第 4 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受付開始から今四半期までの累計件数を示しています。

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	**35** 件	**580** 件
ウェブサイト	**259** 件	**3,855** 件
合計	**294** 件	**4,435** 件

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 4 四半期に JVN で対策情報を公表したものは 35 件（累計 580 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 35 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 15 件と最も多く、次いで「サービス運用妨害」が 4 件です（別紙 2 表 1-3 参照）。

今四半期に対策情報を公表した 35 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 5 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。**

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 4 四半期に修正を完了したものは 259 件（累計 3,855 件）でした。修正を完了した 259

件の対策内容の内訳は、ウェブアプリケーションを修正したものが 244 件（94%）、当該ページを削除したものが 15 件（6%）でした。なお、修正を完了した 259 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. ソフトウェア製品の脆弱性関連情報に関する届出の傾向

～スマートフォンに関連する届出が増加傾向～

2011 年のソフトウェア製品に関する脆弱性関連情報の届出について、届出されるソフトウェア製品の傾向が変化してきています。図 6 は、2011 年のソフトウェア製品の届出全体のうち、スマートフォン関連の届出が占める割合を示しています。2011 年においては、全体の 22%がスマートフォン関連の届出でした。図 7 は、2011 年のソフトウェア製品（OS およびアプリケーション）の届出について、スマートフォンに関連するものの割合を四半期ごとに示しています。2011 年第 1 四半期、第 2 四半期においては、スマートフォンに関連したソフトウェア製品の届出の割合は 10%未満でしたが、第 3 四半期は約 30%、第 4 四半期は約 40%と急増しています。

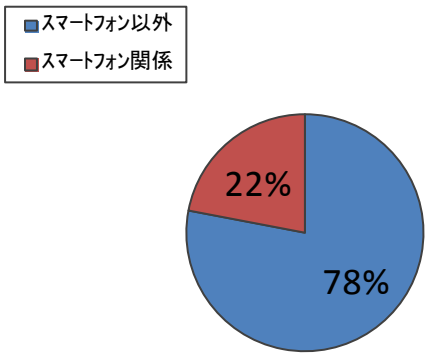


図6. ソフトウェア製品の届出状況（2011年）

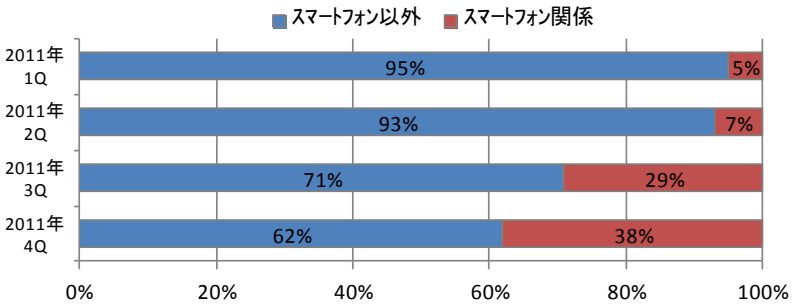


図7. ソフトウェア製品の届出状況（四半期毎）

スマートフォンに関連するソフトウェア製品の開発者には、脆弱性が発見された際の速やかな対応を期待します。

4. ウェブサイトの脆弱性関連情報に関する届出の傾向

～見落としやすい「クロスサイト・スクリプティング」の脆弱性対策～

2011 年のウェブサイトに関する脆弱性関連情報の届出について、「クロスサイト・スクリプティング」の件数が 619 件となり、全体の 91%を占めました。

図 8 は、ウェブサイトに関する脆弱性の届出（不受理を除く）のうち、2010 年と 2011 年の脆弱性の種類が「クロスサイト・スクリプティング」の件数を示したものです。2011 年は「クロスサイト・スクリプティング」の届出が急増し、「その他」の脆弱性の届出は減少しています。

図 9 は 2011 年に届出のあった「クロスサイト・スクリプティング」の脆弱性について、問題箇所の割合を示したものです。テキスト欄のようなブラウザから直接文字列を入力できる箇所 (*3) に脆弱性が存在する割合は 66%、チェック項目欄や隠し要素のようなブラウザからは直接文字列を入力できない箇所 (*4) は 34%でした。

直接入力ができない箇所に脆弱性が確認されたウェブサイト 34%（213 件）のうちの 5%（32 件）分は、過去にも同じ「クロスサイト・スクリプティング」の届出があったウェブサイトでし

(*3) type 属性値が「text」である input 要素等
(*4) type 属性値が「hidden」や「checkbox」である input 要素等

た。過去に届出があった箇所以外について、脆弱性の見直し作業が不十分であったため、再度別の箇所に脆弱性が確認されたものと推測されます。

「クロスサイト・スクリプティング」の脆弱性対策については、テキスト欄のようなブラウザから文字列を直接入力できる箇所の対策だけではなく、チェック項目欄や隠し要素のようなブラウザから文字列を直接入力できない箇所の対策も必要です。

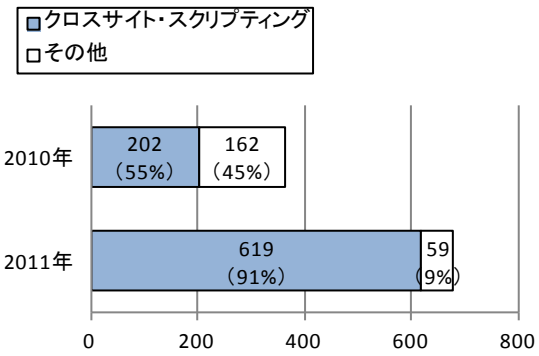


図8. 脆弱性の種類別の届出件数の割合（過去2年間）

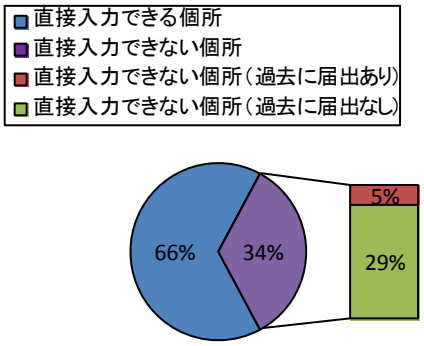


図9. 脆弱性の存在箇所別の割合と過去の届出有無（2011年）

ウェブサイト運営者が「クロスサイト・スクリプティング」の脆弱性対策を実施する際は、ブラウザから文字列を直接入力できない箇所への対策が取られているかを確認してください。

また、届出で指摘された箇所以外にも脆弱性がないか、全体的な見直しを行ってください。

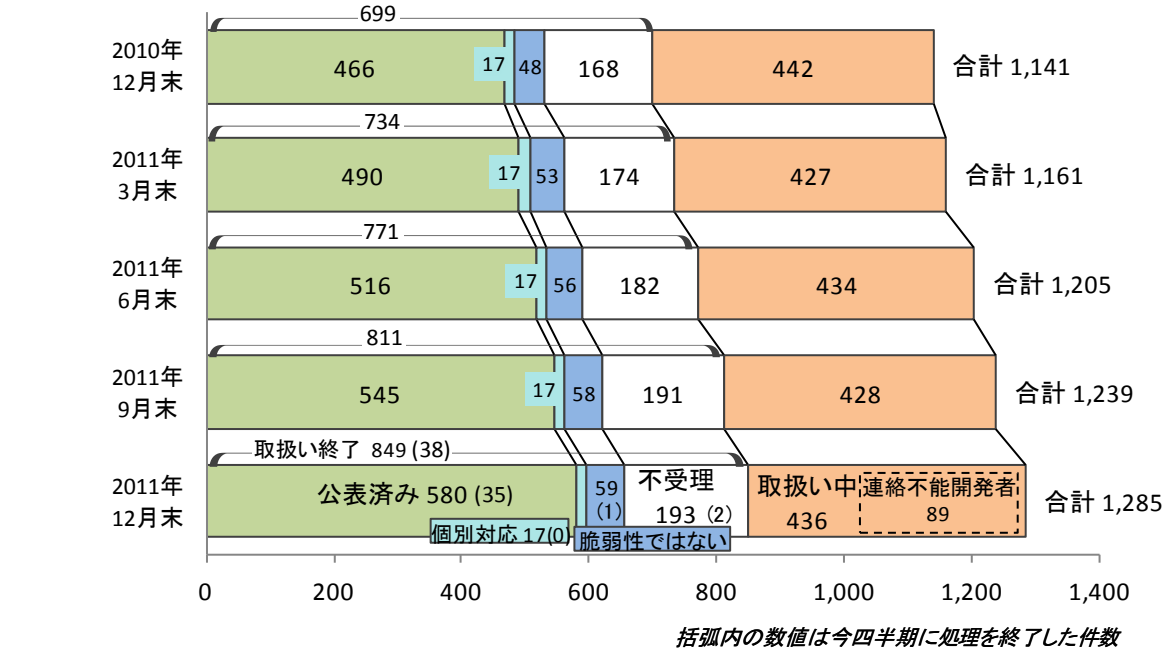
別紙 2

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 35 件（累計 580 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 1 件（累計 59 件）、「不受理」としたものは 2 件 [*5]（累計 193 件）、取扱い中は 436 件です。取扱中の届出のうち 49 件（累計 89 件）については製品開発者と連絡が取れないことから、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るため、連絡不能開発者一覧に掲載しました。



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
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
連絡不能開発者	：	連絡不能開発者一覧に掲載したもの

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 1,285 件のうち、不受理を除いた 1,092 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「ウェブブラウザ」が前四半期と比較して約 4 倍に増加しています。

[*5] 前四半期までの届出の中で今四半期に不受理とした 2 件です。

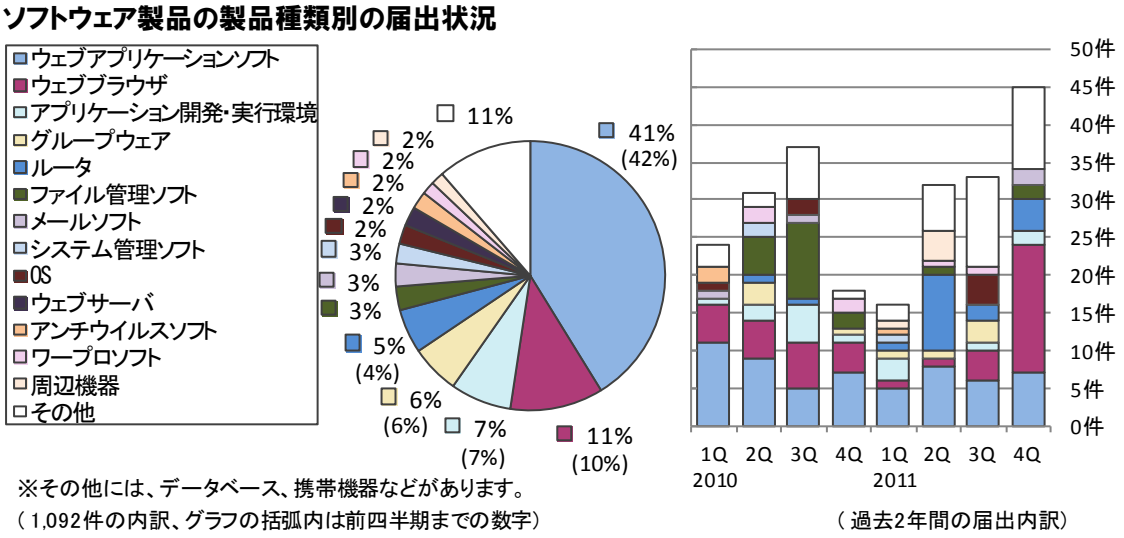


図1-2. 製品種類別の届出件数の割合　**図1-3. 製品種類別の届出件数（四半期別推移）**

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 1,285 件のうち、不受理のものを除いた 1,092 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 33%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。

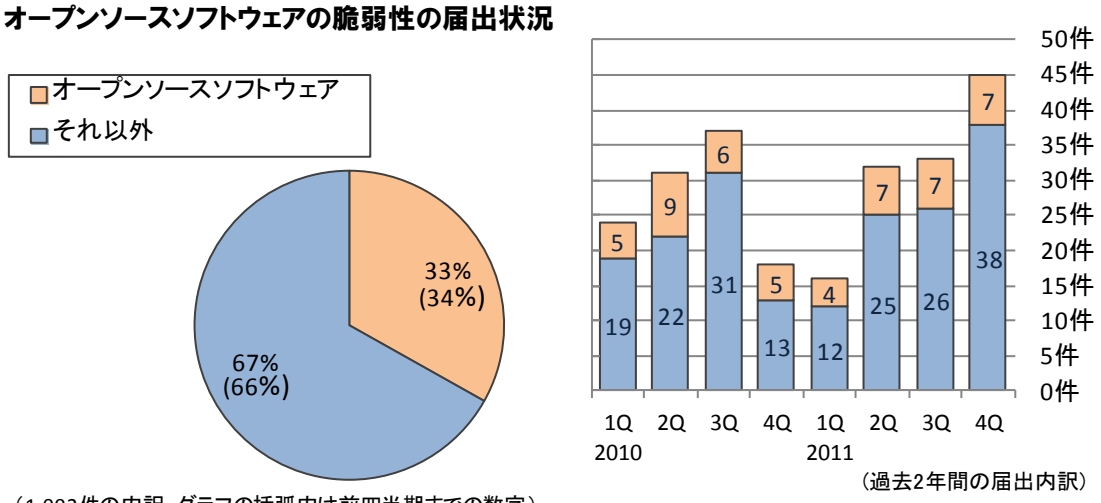


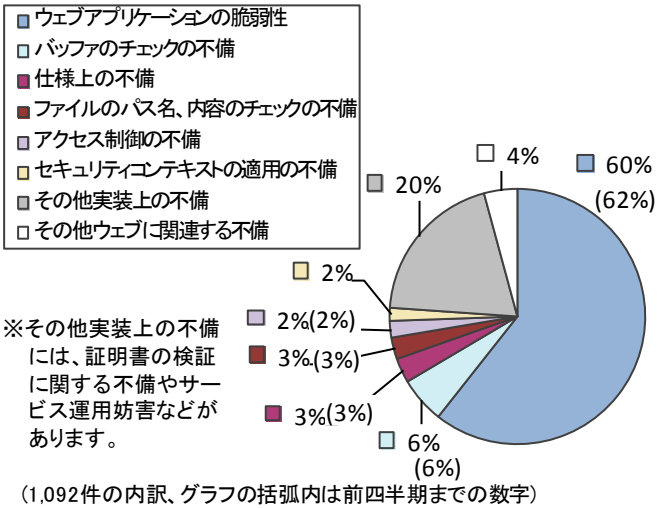
図1-4. オープンソースソフトウェアの届出件数の割合　**図1-5. オープンソースソフトウェアの届出件数（四半期別推移）**

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 1,285 件のうち、不受理のものを除いた 1,092 件について、図 1-6 のグラフは原因別[*6]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。今四半期におけるソフトウェア製品の脆弱性の原因は「その他実装上の不備」が最多となっています。

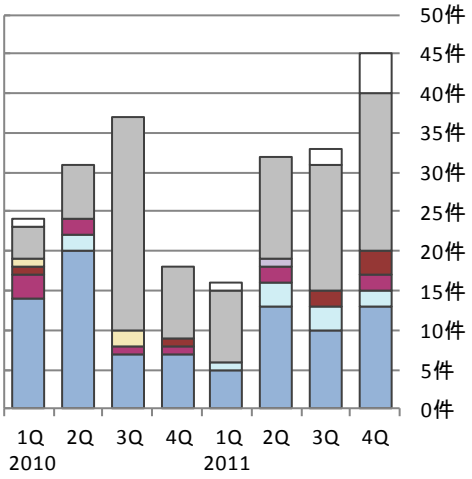
[*6] それぞれの詳しい脆弱性の原因の説明については付表 1 を参照してください。

ソフトウェア製品の脆弱性の原因別の届出状況



（1,092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

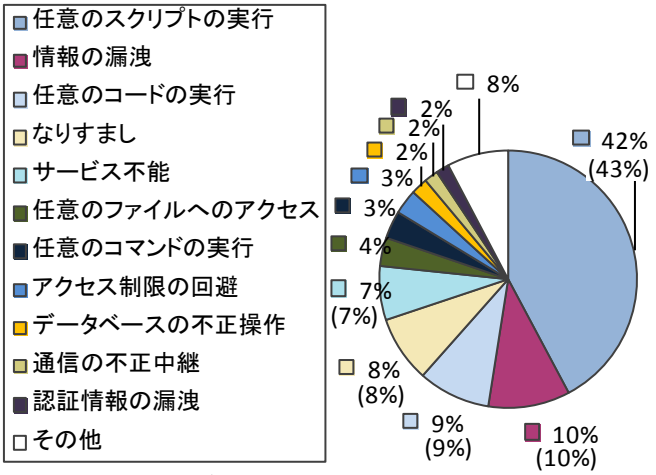


（過去2年間の届出内訳）

図1-7. 脆弱性の原因別の届出件数（四半期別推移）

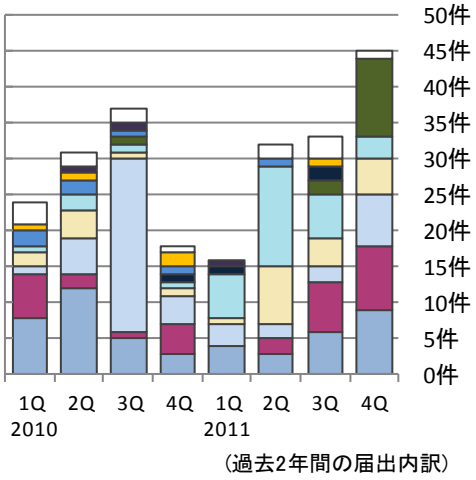
図 1-8 のグラフは脆弱性がもたらす脅威別の届出件数の割合を、図 1-9 は過去 2 年間の脆弱性がもたらす脅威別届出件数の四半期別推移をそれぞれ示したものです。脆弱性がもたらす脅威は「任意のスクリプト実行」が半数近くを占めています。また、今四半期は「任意のファイルへのアクセス」が急増しています。

ソフトウェア製品の脆弱性がもたらす脅威別の届出状況



（1,092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受付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[*7]。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 1,303 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。

[*7] JPCERT/CC 活動概要 Page15~22（https://www.jpcert.or.jp/pr/2012/PR20120112.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	35 件	580 件
②	海外 CSIRT 等と連携して公表したもの	44 件	723 件
	合計	79 件	1,303 件

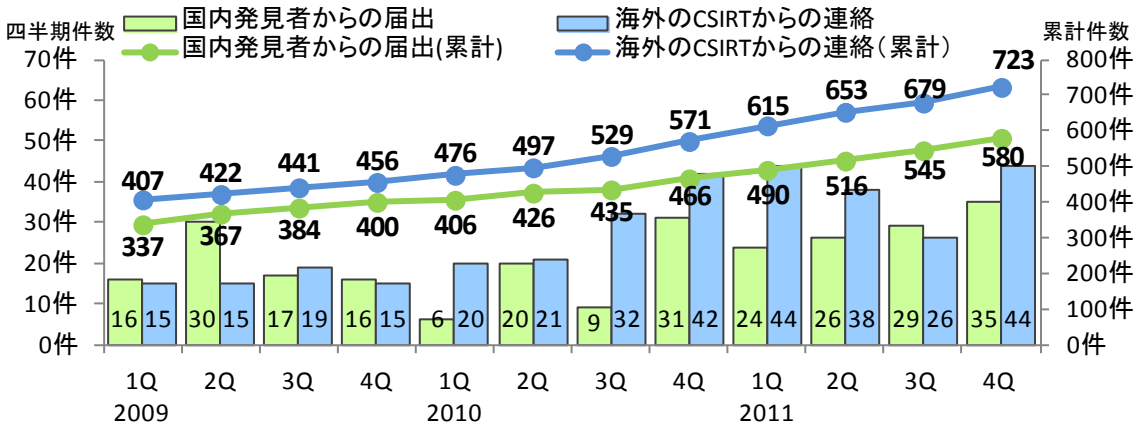


図1-10. ソフトウェア製品の脆弱性対策情報の公表件数

(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 4 四半期で 33%、45 日を超過した件数は 64%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。

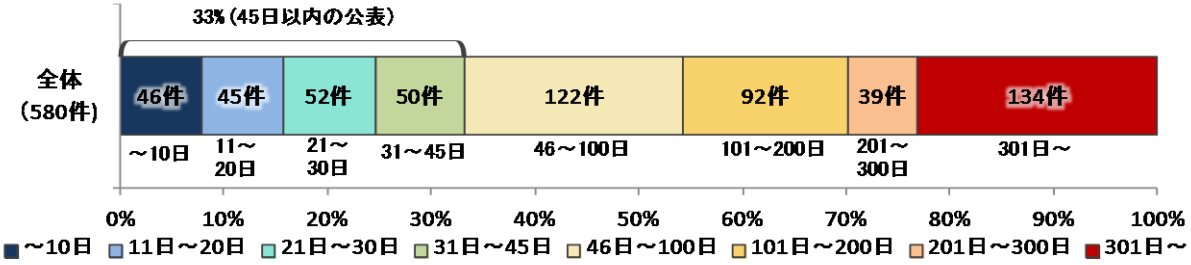


図1-11. ソフトウェア製品の脆弱性公表日数

表 1-2. 45 日以内に公表した件数の割合推移（四半期別）

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

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 14 件（表 1-3 の*1）、組込みソフトウェア製品の脆弱性が 4 件（表 1-3 の*2）、制御システムの脆弱性が 1 件（表 1-3 の*3）ありました。

表 1-3. 2011 年第 4 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 III（危険）、CVSS 基本値=7.0～10.0				
1 (*2)	複数の D-Link 製品におけるバッファオーバーフローの脆弱性	複数の D-Link 製品には、バッファオーバーフローの問題がありました。このため、遠隔の第三者によって任意のコードを実行される可能性がありました。	2011 年 10 月 28 日	10.0
2	ＨＰの回し者製「日記」における OS コマンド・インジェクションの脆弱性	日記ソフトウェア「日記」には、OS コマンド・インジェクションの問題がありました。このため、第三者によって任意のコマンドを実行される可能性がありました。	2011 年 11 月 21 日	7.5
3	Preboot Execution Environment (PXE) SDK を使用した製品における複数の脆弱性	Preboot Execution Environment (PXE) SDK のサンプルコードを利用している製品に、ディレクトリ・トラバーサルおよびバッファオーバーフローの問題がありました。このため、第三者によって任意のコードを実行されるなどの可能性がありました。	2011 年 12 月 15 日	8.3
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
4 (*1)	「宴会くん」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「宴会くん」には、ウェブ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、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 10 月 7 日	5.0
5 (*1)	「A-Form」におけるアクセス制限不備の脆弱性	Movable Type のプラグイン「A-Form」には、アクセス制限不備の問題がありました。このため、第三者により A-Form 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 10 月 7 日	4.0
6	「サイボウズ Office」におけるアクセス制限不備の脆弱性	グループウェアソフト「サイボウズ Office」には、アクセス制限不備の脆弱性がありました。このため、当該システムにログインしたユーザによって任意のユーザの勤怠情報を閲覧される可能性がありました。	2011 年 10 月 7 日	4.0
7	「WEB FORUM」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「WEB FORUM」には、ウェブページを出力する際の処理に問題がありました。項番 8, 32 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。	2011 年 10 月 11 日	5.0
8	「WEB FORUM」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「WEB FORUM」には、ウェブページに出力する際の処理に問題がありました。項番 7, 32 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。	2011 年 10 月 11 日	4.3
9 (*1)	「Pligg」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「Pligg」には、ウェブページに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スクリプトを埋め込まれる可能性がありました。	2011 年 10 月 13 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
10	「DAEMON Tools」におけるサービス運用妨害 (DoS) の脆弱性	ディスクイメージ作成ツール「DAEMON Tools」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、システムにログインできる第三者によって、そのシステムをクラッシュさせられる可能性がありました。	2011 年 10 月 13 日	4.9
11 (*1)	「DBD::mysqlPP」における SQL インジェクションの脆弱性	MySQL 接続用ライブラリ「DBD::mysqlPP」には、SQL 文を組み立てる処理に問題がありました。このため、ウェブアプリケーションが SQL インジェクション対策をしていたとしても、対策を迂回される可能性がありました。	2011 年 10 月 14 日	6.8
12 (*1)	「EC-CUBE」における SQL インジェクションの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」には、利用者から入力された内容をもとに SQL 文を組み立てる処理に問題がありました。このため、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 10 月 14 日	5.0
13 (*1)	「FFFTP」における実行ファイル読み込みに関する脆弱性	FTP クライアント「FFFTP」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。項番 25 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 10 月 28 日	5.1
14	「東方緋想天」におけるサービス運用妨害 (DoS) の脆弱性	PC 用のゲームソフト「東方緋想天」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、遠隔の第三者によって、当該製品が異常終了させられる可能性がありました。	2011 年 10 月 28 日	5.0
15	複数のスカイアークシステム製品におけるアクセス制限不備の脆弱性	株式会社スカイアークシステムが提供する MTCMS や複数の Movable Type 用のプラグインには、アクセス制限不備の問題が存在しました。このため、システムにログインできる第三者によって、設定を変更されたり、ファイルを改ざんされたりする可能性がありました。	2011 年 10 月 31 日	4.0
16 (*3)	「CSWorks」の LiveData Service におけるサービス運用妨害 (DoS) の脆弱性	産業オートメーション用システム「CSWorks」の LiveData Service 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、第三者によって、サービス運用妨害 (DoS) 攻撃を受ける可能性がありました。	2011 年 11 月 1 日	5.0
17 (*2)	複数の Opengear 製品における認証回避の脆弱性	Opengear 社が提供する複数のコンソールサーバ製品には、認証回避の脆弱性が存在しました。このため、第三者によって、設定を変更されたり、接続されている機器にアクセスされる可能性がありました。	2011 年 11 月 4 日	6.4
18	「WebObjects」におけるクロスサイト・スクリプティングの脆弱性	アプリケーションサーバ「WebObjects」には、ウェブ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、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 11 月 4 日	4.3
19	「いわてポータルバー」において任意のスクリプトが実行される脆弱性	ブラウザ機能拡張ソフト「いわてポータルバー」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。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る可能性がありました。	2011 年 11 月 8 日	4.3
20	「茶筌 (ChaSen)」におけるバッファオーバーフローの脆弱性	日本語の形態素解析をするソフトウェア「茶筌 (ChaSen)」には、バッファオーバーフローの脆弱性がありました。このため、遠隔の第三者によって、任意のコードを実行される可能性がありました。	2011 年 11 月 8 日	6.8

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	ＨＰの回し者製「日記」におけるディレクトリ・トラバーサルの脆弱性	日記ソフトウェア「日記」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、第三者によりサーバ内のファイルを閲覧される可能性がありました。	2011 年 11 月 21 日	5.0
22	「PowerChute Business Edition」におけるクロスサイト・スクリプティングの脆弱性	UPS 管理ソフトウェア「PowerChute Business Edition」には、ウェブ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、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 12 月 2 日	4.3
23 (*1)	「Etomite」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「Etomite」には、ウェブ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、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 12 月 6 日	4.3
24	「phpWebSite」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「phpWebSite」には、ウェブ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、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 12 月 8 日	4.3
25 (*1)	「FFFTP」における実行ファイル読み込みに関する脆弱性	FTP クライアント「FFFTP」には、ファイルの読み込み処理に問題があり、実行ファイルなどの意図しないファイルを読み込んでしまう脆弱性が存在しました。項番 13 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 12 月 9 日	5.1
26 (*2)	iOS 上の「Safari」におけるサービス運用妨害 (DoS) の脆弱性	iOS 上のウェブブラウザ「Safari」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、第三者によって、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 12 月 15 日	4.3
27 (*1)	「Apache Struts」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フレームワーク「Apache Struts」には、ウェブ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、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 12 月 22 日	4.3
28 (*1)	「PukiWiki Plus!」におけるクロスサイト・スクリプティングの脆弱性	Wiki 機能を提供するソフトウェア「PukiWiki Plus!」には、ウェブ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、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 12 月 22 日	4.3
29 (*1)	Movable Type 用「メールフォームプラグイン」におけるクロスサイト・スクリプティングの脆弱性	Movable Type 用プラグイン「メールフォームプラグイン」には、ウェブ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、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 12 月 26 日	4.3
30 (*1)	「WordPress」において任意の PHP コードが実行可能な脆弱性	ウェブログシステム「WordPress」には、任意の PHP コードが実行可能な問題がありました。このため、第三者により製品が持つ権限で任意の PHP コードが実行される可能性が可能性がありました。	2011 年 12 月 26 日	6.5
31 (*1)	「WordPress 日本語版」におけるクロスサイト・スクリプティングの脆弱性	ウェブログシステム「WordPress 日本語版」には、ウェブ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、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 12 月 26 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
脆弱性の深刻度=レベルⅠ（注意）、CVSS 基本値=0.0～3.9				
32	「WEB FORUM」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「WEB FORUM」には、Cookie 情報をウェブページに出力する際の処理に問題がありました。項番 7, 8 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。	2011 年 10 月 11 日	2.6
33 (*1)	「Plume」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「Plume」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 10 月 13 日	2.6
34 (*2)	iOS 上の「Safari」におけるクロスサイト・スクリプティングの脆弱性	iOS 上のウェブブラウザ「Safari」には、HTTP Content-Disposition ヘッダの処理に問題がありました。このため、ウェブサイト側でクロスサイト・スクリプティング対策をしていた場合でも、対策を迂回される可能性がありました。	2011 年 10 月 17 日	2.6
35	複数のスカイアークシステム製品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	株式会社スカイアークシステムが提供する MTCMS や複数の Movable Type 用のプラグインには、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、第三者により MTCMS 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 10 月 31 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
（*3）：制御システムの脆弱性

（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 44 件あり、うち表 1-4 には通常の脆弱性情報 39 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 [*8] 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	ProjectForum における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
2	SlimPDF Reader に複数の脆弱性	注意喚起として掲載
3	Iceni Argus 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
4	UPnP 対応の複数のルータにアクセス制限不備の脆弱性	注意喚起として掲載 複数製品開発者へ通知
5	GoAhead Webserver 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	D-Link DIR-685 Xtreme N Storage Router の暗号化通信に脆弱性	注意喚起として掲載
7	Apple iTunes 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
8	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
9	Apple TV 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
10	Apple Mac OS X 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
11	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
12	VLC Media Player に脆弱性	注意喚起として掲載
13	BlueZ-hcidump におけるヒープオーバーフローの脆弱性	注意喚起として掲載
14	OneOrZero AIMS に複数の脆弱性	注意喚起として掲載
15	MIT Kerberos 5 KDC に複数の脆弱性	注意喚起として掲載
16	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
17	Enspire eClient に SQL インジェクションの脆弱性	注意喚起として掲載
18	NJStar Communicator 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	Microsoft Windows の TrueType フォント解析処理に脆弱性	注意喚起として掲載
20	Java for Mac OS 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
21	eEye Retina CS Vulnerability Management Console が任意のプログラムを実行する問題	注意喚起として掲載
22	Aviosoft DTV Player 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
23	Dell KACE K2000 System Deployment Appliance に不正ログイン可能な脆弱性	注意喚起として掲載
24	Dell KACE K2000 System Deployment Appliance に情報漏えいの脆弱性	注意喚起として掲載
25	Dell KACE K2000 System Deployment 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
26	Dell KACE K2000 System Deployment Appliance にコマンドインジェクションの脆弱性	注意喚起として掲載
27	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
28	Apple Time Capsule および AirPort Base Station (802.11n) 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
29	Apple iTunes 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

[*8] 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。

項番	脆弱性	対応状況
30	Zenprise Device Manager 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
31	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
32	Support Incident Tracker に複数の脆弱性	注意喚起として掲載
33	CA SiteMinder 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 複数製品開発者へ通知
34	HomeSeer HS2 に複数の脆弱性	注意喚起として掲載
35	Adobe Reader および Acrobat にメモリ破損の脆弱性	緊急案件として掲載
36	Hewlett-Packard 製品のリモートアップデート機能に脆弱性	注意喚起として掲載
37	JasPer 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
38	Power2Go 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
39	Unbound にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載

表 1-5.米国 US-CERT (*9) 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	Apple Mac OS X 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	Microsoft 製品における複数の脆弱性に対するアップデート
5	Adobe 製品における複数の脆弱性

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

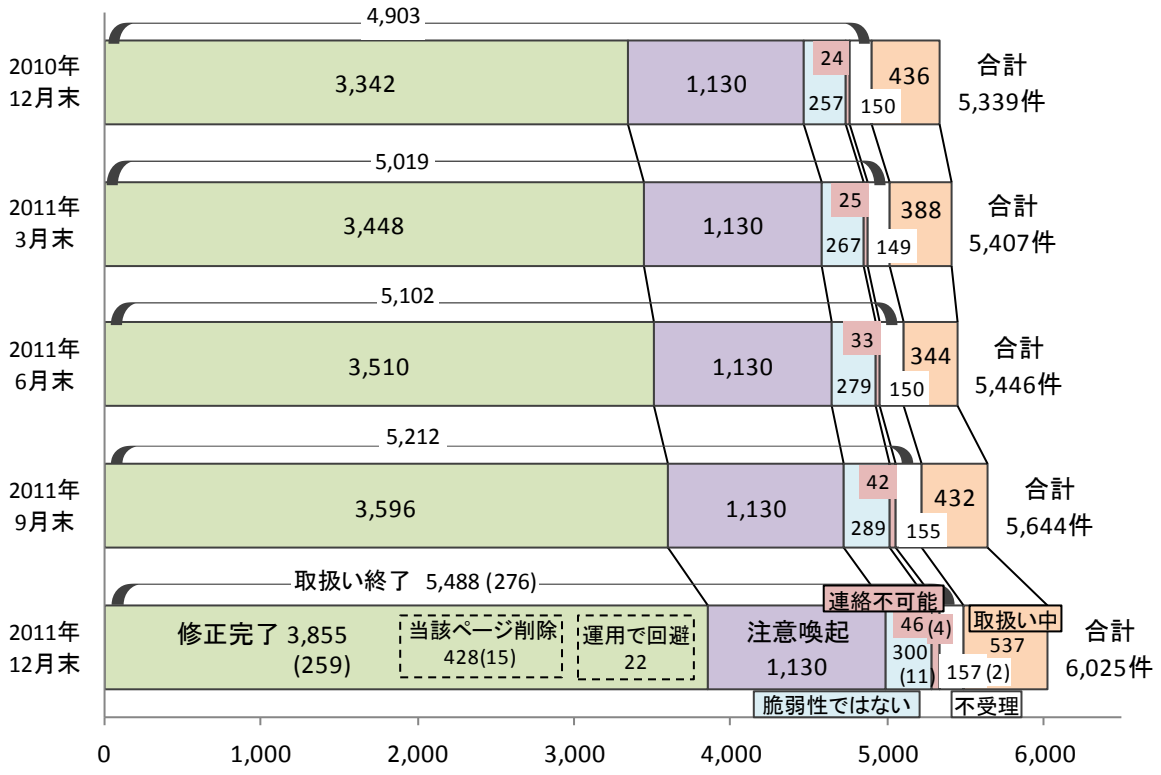
2. ウェブサイトの脆弱性の処理状況の詳細

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 276 件（累計 5,488 件）でした。このうち「修正完了」したものは 259 件（累計 3,855 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 11 件（累計 300 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 4 件（累計 46 件）です。「不受理」としたものは 2 件（累計 157 件）でした。

取扱いを終了した累計 5,488 件のうち「注意喚起」「連絡不可能」「不受理」を除く累計 4,155 件（76%）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 15 件（累計 428 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

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。

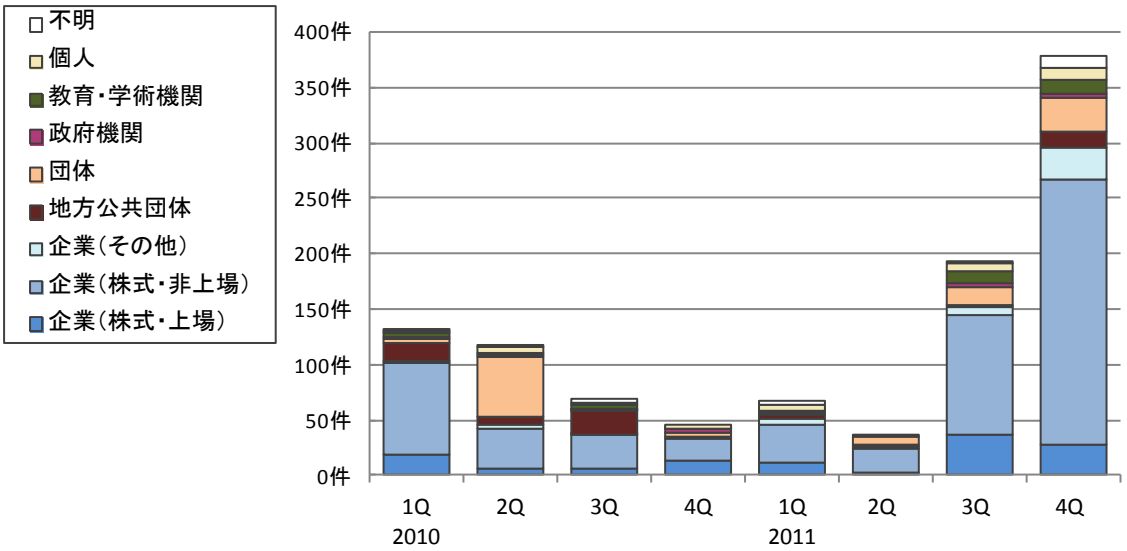
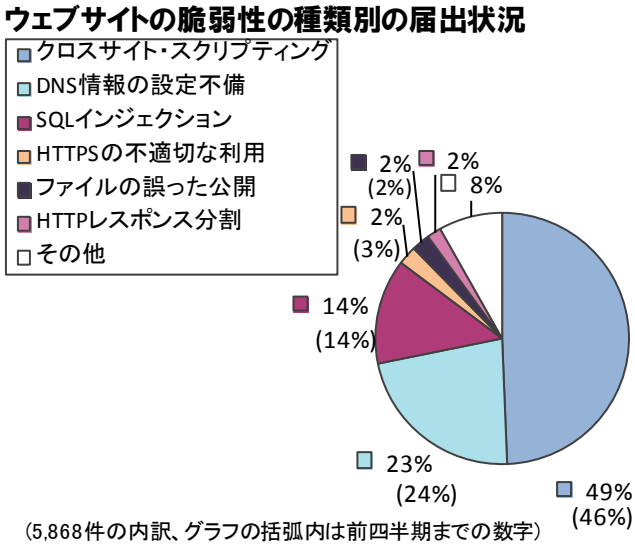


図2-2. ウェブサイトの運営主体の種類別の届出件数（四半期別推移）

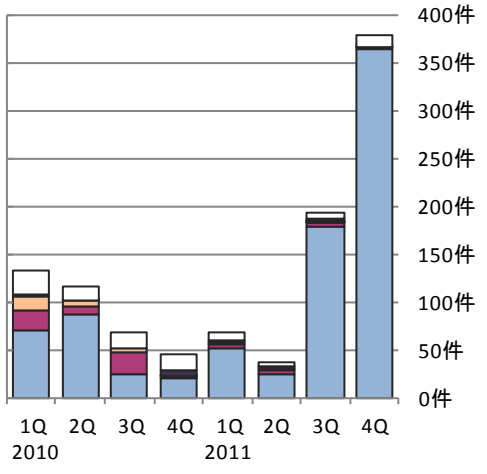
2.3 ウェブサイトの脆弱性の種類と脅威

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 6,025 件のうち、不受理のものを除いた 5,868 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 86%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（379 件）のうち、「クロスサイト・スクリプティング」だけで 96%（364 件）を占めます。



（5,868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

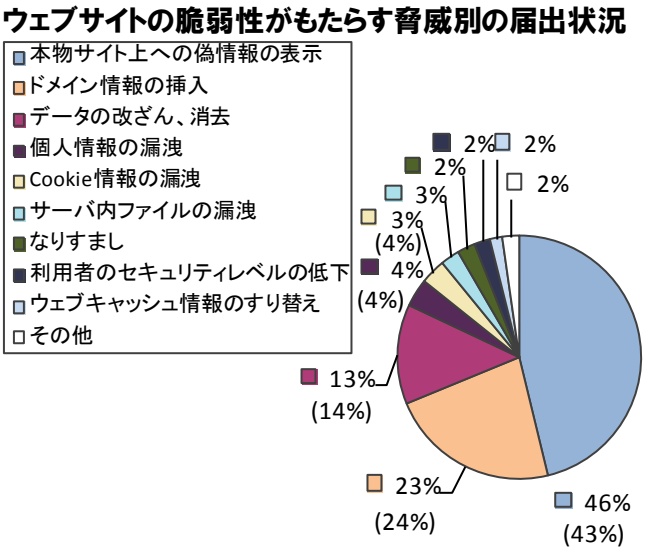


（過去2年間の届出内訳）

図2-4. 脆弱性の種類別の届出件数（四半期別推移）

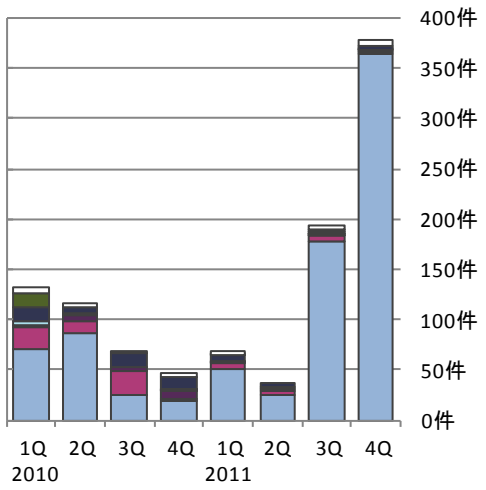
[*10] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

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 82%を占めています。



(5,868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。今四半期は「0-90 日以内」の件数が急増しています。これは、届出の急増に伴い、ウェブサイト運営者に多くの脆弱性関連情報を送付し、ウェブサイト運営者が迅速に対応したためです。

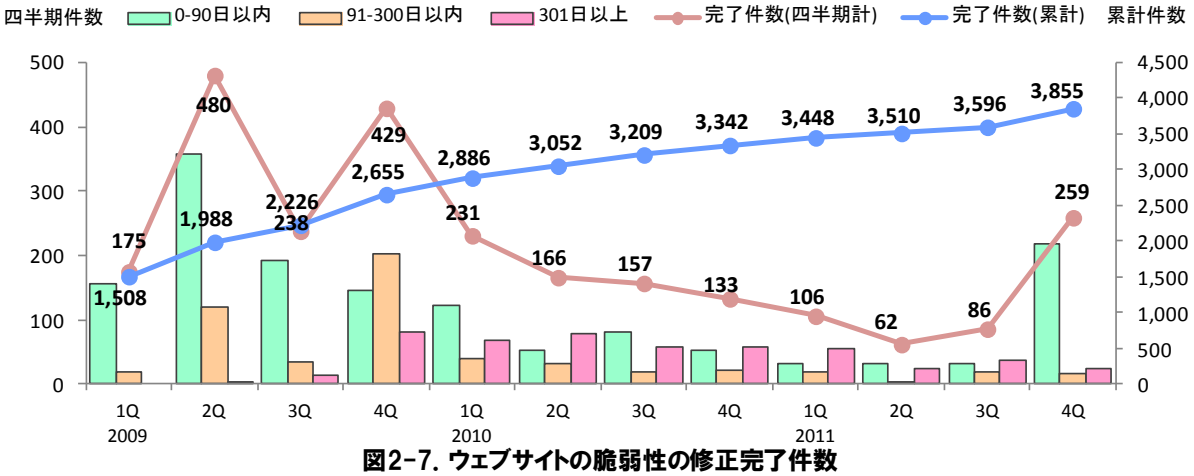


図2-7. ウェブサイトの脆弱性の修正完了件数

表 2-1. 90 日以内に修正完了した件数および割合の推移

	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q
修正完了件数	1,508	1,988	2,226	2,655	2,886	3,052	3,209	3,342	3,448	3,510	3,596	3,855
90 日以内の件数	1,212	1,569	1,760	1,905	2,028	2,082	2,163	2,216	2,247	2,280	2,311	2,528
90 日以内の割合	80%	79%	79%	72%	70%	68%	67%	66%	65%	65%	64%	66%

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 47%の届出が 30 日以内、全体の 66%の届出が 90 日以内に修正されています。

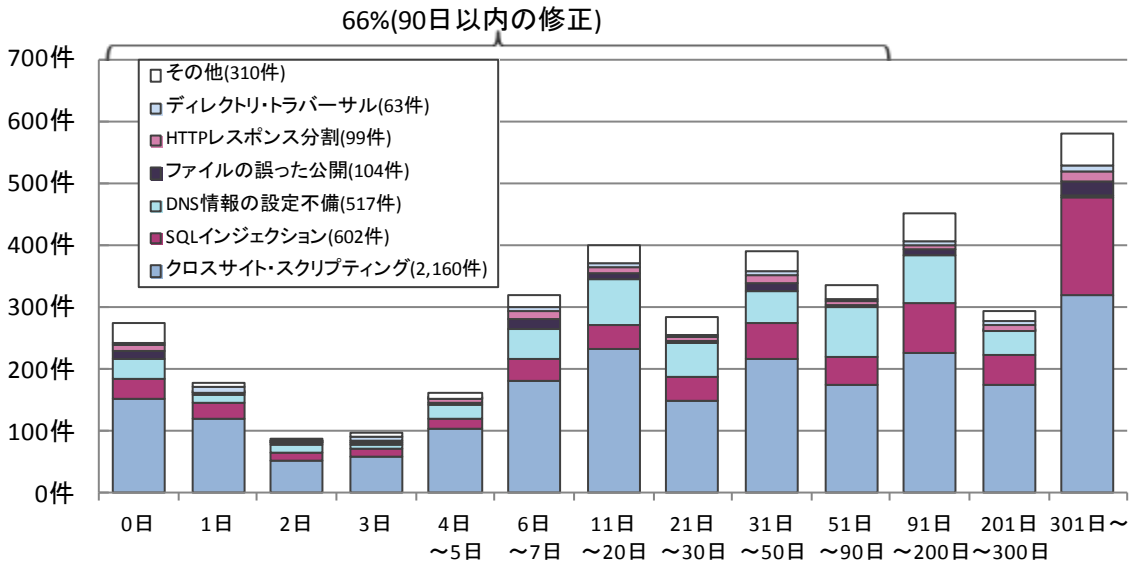


図2-8.ウェブサイトの修正に要した日数

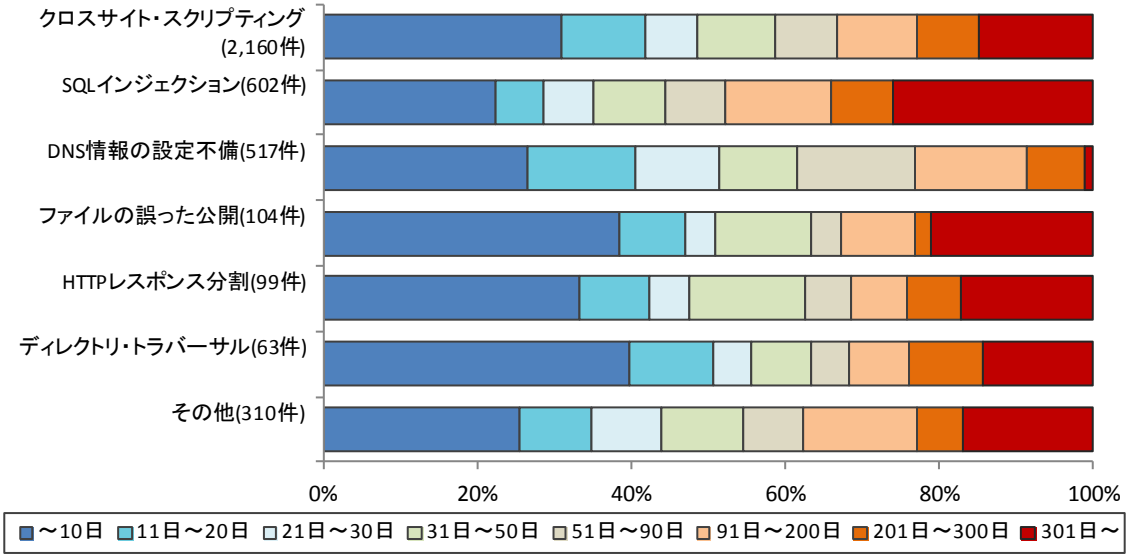


図2-9.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*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 35 件、200 日から 299 日のものは 8 件など、これらの合計は 237 件（前四半期は 228 件）です。前四半期末までの取扱い長期化 228 件のうち今四半期に 25 件が取扱い終了となった一方、新たに 34 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 9 件増加しました。

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、前四半期から、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。

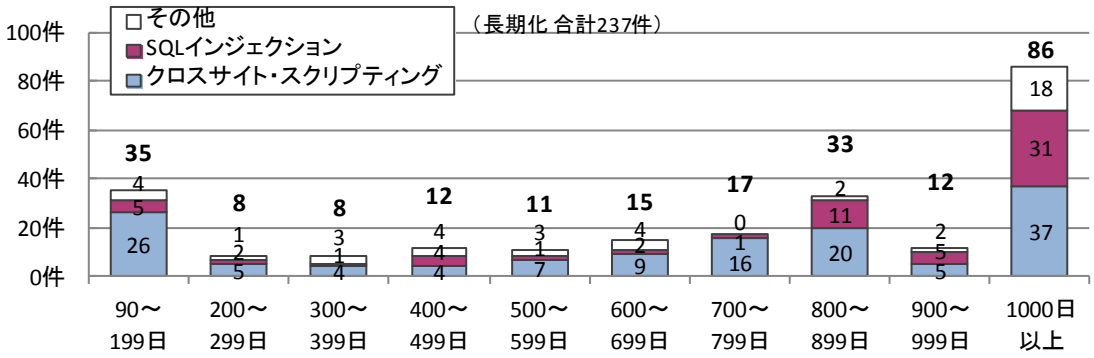


図2-10.取扱いが長期化（90日以上経過）しているウェブサイトの経過日数と脆弱性の種類

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

	2010 1Q	2Q	3Q	4Q	2011 1 Q	2Q	3Q	4Q
取扱い中件数	709 件	653 件	536 件	436 件	388 件	344 件	432 件	537 件
長期化している件数	507 件	440 件	394 件	359 件	309 件	289 件	228 件	237 件
長期化している割合	72%	67%	74%	82%	80%	84%	53%	44%

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

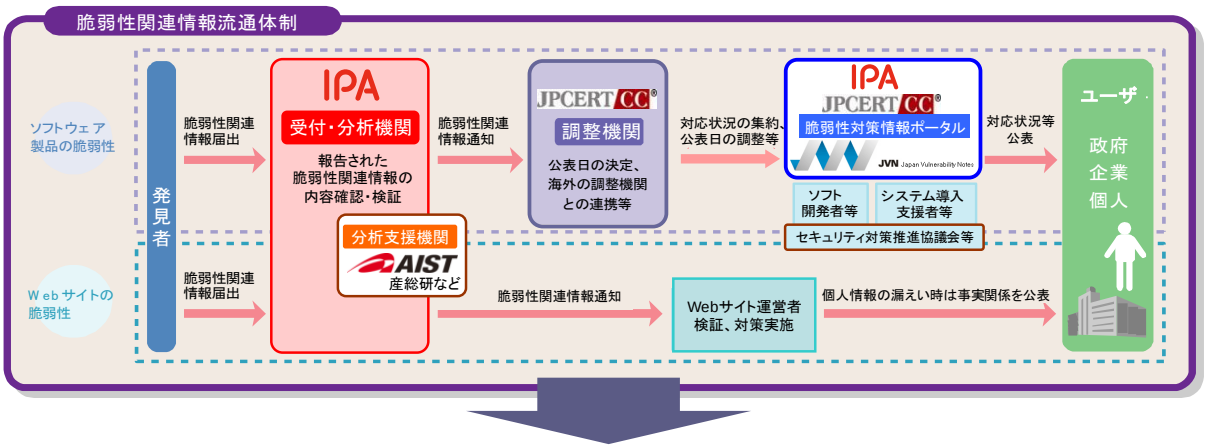
付表 2. ウェブサイト脆弱性の分類

	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