プレスリリース

2011 年 4 月 20 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 1 四半期（1 月～3 月）]

～ウェブサイト運営者は携帯電話向けウェブサイトにおける認証方式の脆弱性の見直しを～

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 1 四半期（1 月～3 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 6,570 件に（別紙 1　1.参照）

2011 年第 1 四半期の IPA への脆弱性関連情報の届出件数は 87 件です。内訳は、ソフトウェア製品に関するものが 19 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 68 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 1,164 件、ウェブサイトに関するものが 5,406 件、合計 6,570 件となりました。

（2）脆弱性の修正完了件数の累計が 3,900 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 1 四半期に JVN (*2) で対策情報を公表したものは 24 件（累計 490 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 1 四半期に修正を完了したものは 107 件（累計 3,449 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 3,939 件となりました。

（3）携帯電話向けウェブサイトにおける認証方式の脆弱性の見直しを（別紙 1　4.参照）

携帯電話向けウェブサイト（以降、携帯サイト）における、いわゆる「かんたんログイン」に関する脆弱性が届出られています。2011 年第 1 四半期末の時点で累計 24 件の届出があり、まだ修正されていない取扱中の届出も存在しています。「かんたんログイン」は携帯電話の識別子だけで利用者を認証する方式の一つですが、安全な実装が簡単ではなく、2010 年 10 月にはこの脆弱性が原因の個人情報漏洩事故が発生しました。

IPA としては「かんたんログイン」を採用している携帯サイトのウェブサイト運営者に対し、IPA が公開している「安全なウェブサイトの作り方 改訂第 5 版 (*3)」を参照し、速やかな認証方式見直しの実施を期待しています。

■ 本件に関するお問い合わせ先
IPA 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/

(*3) 「安全なウェブサイトの作り方 改訂第 5 版」2.7.3 携帯 ID の使用に関する注意点
http://www.ipa.go.jp/security/vuln/documents/website_security.pdf（PDF）

別紙 1

2011 年第 1 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 6,570 件になりました ～

表 1 は 2011 年第 1 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 19 件、ウェブアプリケーション（ウェブサイト）に関するもの 68 件、合計 87 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 1,164 件、ウェブサイトに関するもの 5,406 件、合計 6,570 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	**19** 件	**1,164** 件
ウェブサイト	**68** 件	**5,406** 件
合計	**87** 件	**6,570** 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ほぼ同数で推移し、ウェブサイトの届出は前四半期と比較して増加しています。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 1 四半期末で 4.01 件となりました。

表 2. 届出件数（過去 3 年間）

	2008 2Q	3Q	4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q
累計届出件数[件]	2,322	2,885	4,374	5,226	5,655	5,825	5,976	6,147	6,301	6,416	6,483	6,570
1就業日あたり[件/日]	2.39	2.78	3.99	4.53	4.65	4.56	4.47	4.40	4.32	4.22	4.11	4.01

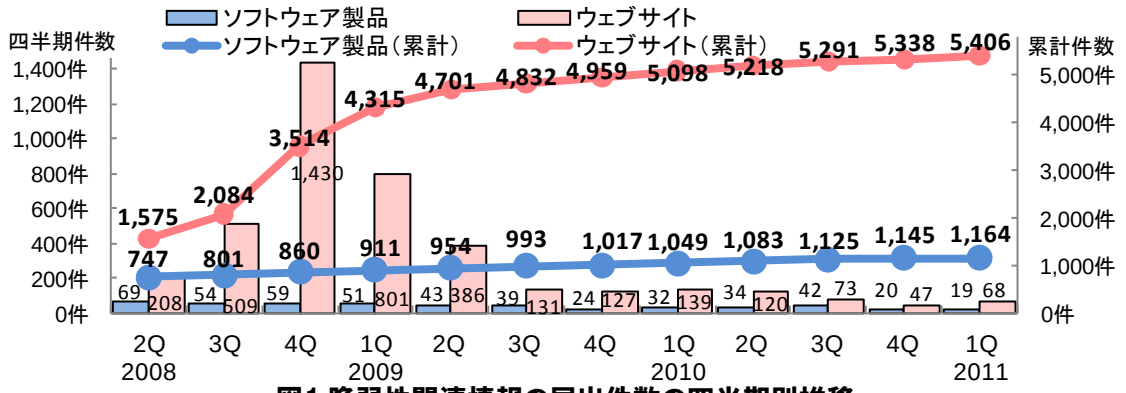


図 1.脆弱性関連情報の届出件数の四半期別推移

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 19 件のうち、不受理を除いた 17 件の製品種類の内訳を、図 3 は脆弱性の脅威の内訳を示したものです。製品の種類は「アプリケーション開発・実行環境」が最も多く、次いで「ウェブアプリケーション」となっています。脆弱性の脅威は「サービス不能」、「任意のスクリプト実行」、「任意のコード実行」が多く届出されており、これらの届出で全体の 8 割強を占めています。

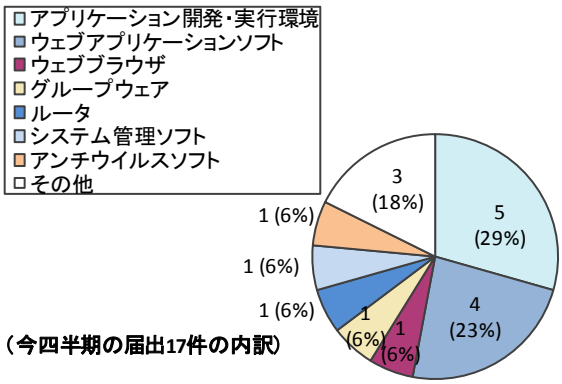


図2. 今四半期のソフトウェア製品種類の内訳

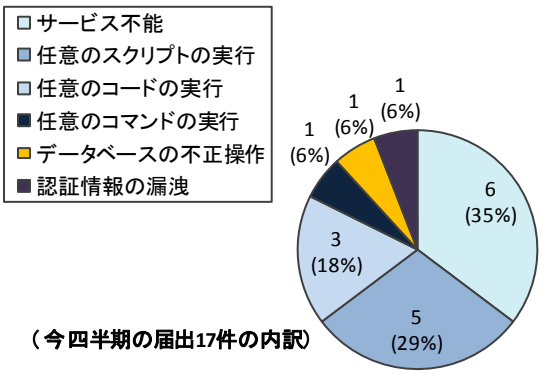


図3. 今四半期の脆弱性の脅威の内訳

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68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75%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、次いで「SQLインジェクション」、「セッション管理の不備」となっています。

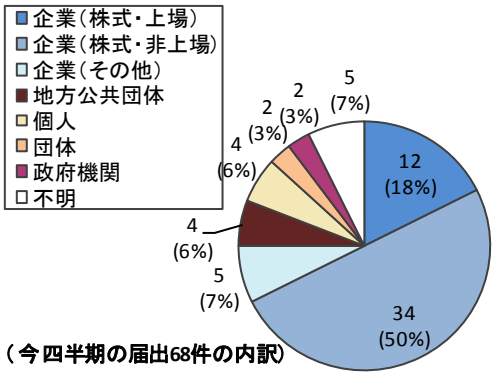


図4. 今四半期のウェブサイト運営主体の内訳

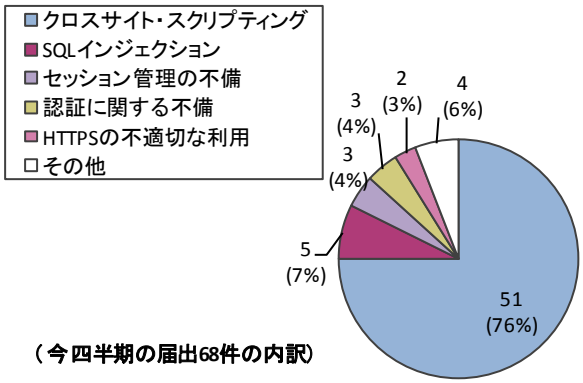


図5. 今四半期の脆弱性の種類の内訳

2.脆弱性の修正完了状況

～　ソフトウェア製品の修正件数が、前四半期と同様に多く、堅調に推移しました　～

表3は2011年第1四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。

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	**24** 件	**490** 件
ウェブサイト	**107** 件	**3,449** 件
合計	**131** 件	**3,939** 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1四半期にJVN [(*1)] で対策情報を公表したものは24件（累計490件）でした。前四半期（31件）に引き続き同じ水準で公表されています。JVNで公表した24件のうち、製品開発者からの届出（自社製品の届出）が5件あり、公表した全件数の21%を占めています。製品開発者からの届出についても、前四半期（16%）と同様高い割合でした。（別紙2 表1-3参照）。**本届出制度は、ソフトウェア製品の利用者に広く脆弱性対策情報を公表するために有効な手段として利用されています。製品開発者には、今後も、自社製品の脆弱性対策情報の周知にJVNを積極的に利用する事を期待します。**

(*1) 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/

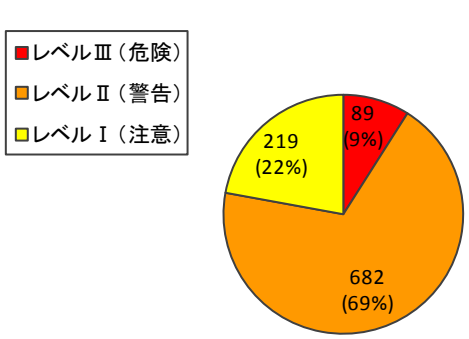
ウェブサイトの脆弱性関連情報の届出に関して、IPA がウェブサイト運営者に通知を行い、2011 年第 1 四半期に修正を完了したものは 107 件（累計 3,449 件）でした。修正完了した 107 件の内訳は、ウェブサイト運営者がウェブサイトを修正したものが 66 件（62%）、当該ページを削除したものが 40 件（37%）、運用で回避したものが 1 件（1%）でした。なお、修正完了した 107 件のうち 76 件（71%）は、届出されてから修正完了まで 1 年以上経過していました。**ウェブサイト運営者による、速やかな対策を期待します。**

3.ソフトウェア製品の脆弱性に関するトピック

～　製品開発者はそれぞれの製品に多く見られがちな脆弱性を作り込まないように　～

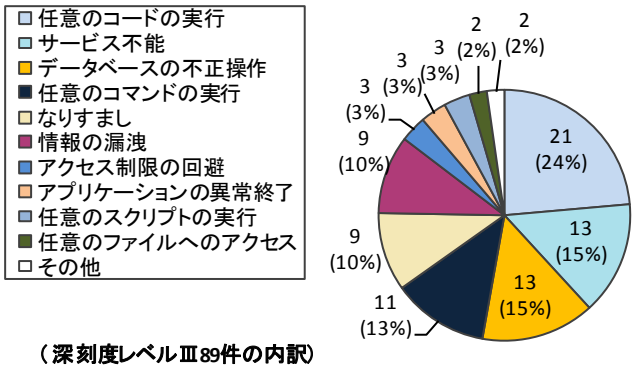
図 6 のグラフは届出受付開始から今四半期までに IPA に届出があったソフトウェア製品に関する脆弱性関連情報 1,164 件のうち、不受理を除いた 990 件の脆弱性の深刻度の内訳です。レベルⅠ(注意)の届出は 219 件(22%)、レベルⅡ(警告)の届出は 682 件(69%)、レベルⅢ(危険)の届出は 89 件(9%)となり、レベルⅡ以上の届出が 8 割近くを占めている状況です。

図 7 のグラフは脆弱性の深刻度がレベルⅢの届出の脆弱性の脅威の内訳です。任意のコード実行が 21 件（24%）、サービス不能が 13 件（15%）、データベースの不正操作が 13 件（15%）、任意のコマンド実行が 11 件（13%）となり、これらの脅威で約 70%を占めている状況です。



（製品の届出990件の内訳）

図6. 製品の脆弱性の深刻度の内訳



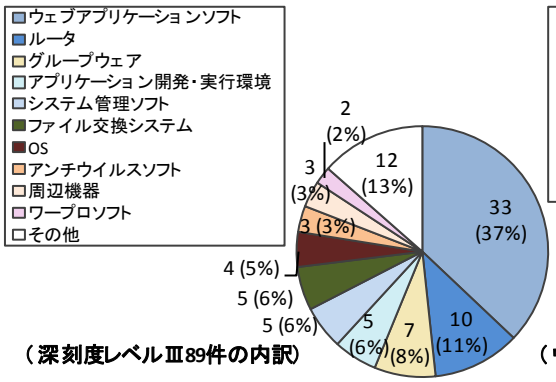
（深刻度レベルⅢ89件の内訳）

図7. 深刻度レベルⅢの脆弱性の脅威の内訳

図 8 のグラフは脆弱性の深刻度がレベルⅢの届出の製品種類の内訳です。レベルⅢの届出が多い製品種類は、ウェブアプリケーションソフトが 33 件（37%）、ルータが 10 件（11%）、グループウェアが 7 件（8%）となり、これらの製品で半数を占めています。

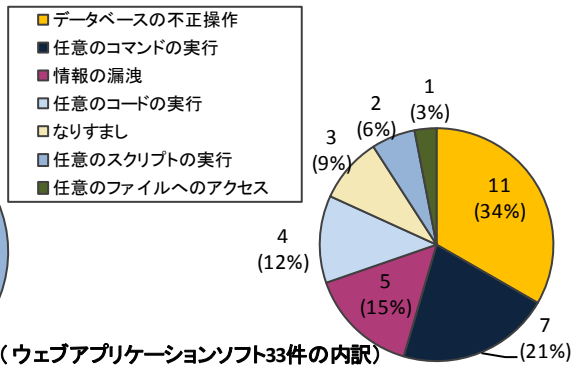
図 9 から図 11 のグラフは深刻度のレベルⅢの届出が多い製品について、どの様な脆弱性の脅威があるかについて、それぞれソフトウェア製品毎の内訳を示します。

図 9 のグラフはウェブアプリケーションソフトのレベルⅢの届出において、どの様な脅威があるのかを示したものです。ウェブアプリケーションソフトの場合は、データベースの不正操作が 11 件（34%）、任意のコマンドの実行が 7 件（21%）、情報の漏洩が 5 件（15%）、任意のコード実行が 4 件（12%）となり、これらの脅威で約 8 割を占めています。



（深刻度レベルⅢ89件の内訳）

図8. 深刻度レベルⅢの製品種類の内訳

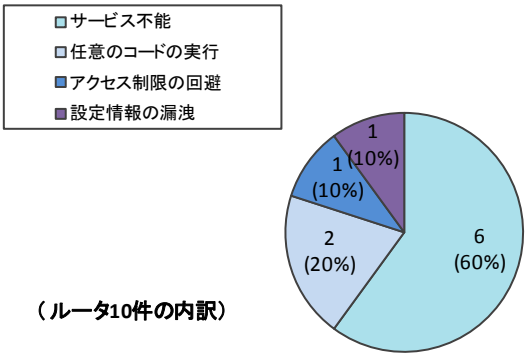


（ウェブアプリケーションソフト33件の内訳）

図9. ウェブアプリケーションソフトの脆弱性の脅威の内訳

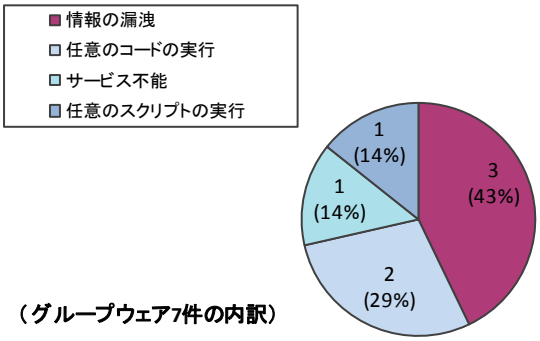
図 10 のグラフはルータ製品のレベルⅢの届出において、どの様な脅威があるのかを示したものです。ルータ製品の場合は、サービス不能が 6 件（60%）、任意のコード実行が 2 件（20%）、アクセス制限の回避が 1 件（10%）、設定情報の漏洩が 1 件（10%）となっています。

図 11 のグラフはグループウェア製品のレベルⅢの届出において、どの様な脅威があるのかを示したものです。グループウェア製品の場合は、情報の漏洩が 3 件（43%）、任意のコードの実行が 2 件（29%）、サービス不能が 1 件（14%）、任意のスクリプトの実行が 1 件（14%）となっています。



（ルータ10件の内訳）

図10. ルータの脆弱性の脅威の内訳



（グループウェア7件の内訳）

図11. グループウェアの脆弱性の脅威別の内訳

これらのソフトウェア製品については、利用者が多く、また多くの製品が流通しています。製品開発者がこれらのソフトウェア製品を開発する場合は、それぞれのソフトウェア製品で多く見られがちな脆弱性を作り込まない様に、ソフトウェアの企画・設計にあたることが必要です。

4.ウェブサイトの脆弱性に関するトピック

～　携帯電話向けウェブサイトにおける認証方式の見直しを　～

2010 年に届出されたウェブサイトの脆弱性関連情報では、携帯電話向けウェブサイト（以降、携帯サイト）における、いわゆる「かんたんログイン」(*2) に関する脆弱性が 19 件報告されました。これらの届出（2010 年以前に報告された 5 件も含む）について、今四半期末時点で、まだ修正されておらず取扱い中の届出も存在している状況です。この脆弱性が悪用されると、個人情報漏洩事故やなりすまし被害につながるため、ウェブサイト運営者による脆弱性の早期な修正を望みます。

「かんたんログイン」は携帯電話やその契約者ごとに割り振られた携帯電話の識別子だけで利用者を認証する方式の一つですが、安全な実装が簡単ではありません (*3)。また 2010 年 10 月には、「かんたんログイン」に関する脆弱性が原因で個人情報漏洩事故が発生しました。

この脆弱性は 2009 年第 3 四半期から報告され始め、それ以降断続的に報告されています（図 12）。2011 年第 1 四半期までに、累計 24 件の届出がありました。この脆弱性が報告されたウェブサイトには、利用者間の情報交換に活用されるブログサービスやソーシャルネットワークサービス（SNS:Social Network Service）、通販サイト（EC サイト）などがあります。これらのようなウェブサイトでは、利便性を高めるために「かんたんログイン」を実装する場合が多く、脆弱性を作り込み易い状況にあるといえます。

「かんたんログイン」を採用している携帯サイトのウェブサイト運営者は、「安全なウェブサイトの作り方 改訂第 5 版」を参照し、「かんたんログイン」に関する脆弱性を認識してください。「かんたんログイン」が必要な場合でも、PC 向けサイトと同様にパスワード等による認証方式を採用することを推奨します。

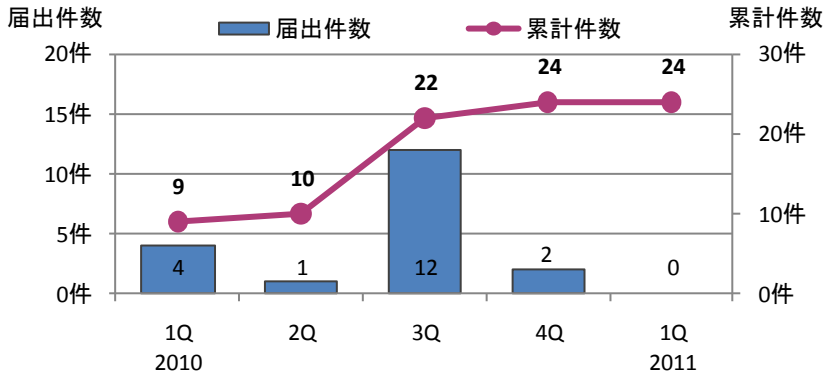


図12.「かんたんログイン」の脆弱性届出件数の推移

(*2) 「簡単ログイン」、「クイックログイン」など類似した呼称があります。本文では「かんたんログイン」という呼称で統一します。

(*3) 「安全なウェブサイトの作り方 改訂第 5 版」2.7.3 携帯 ID の使用に関する注意点
http://www.ipa.go.jp/security/vuln/documents/website_security.pdf（PDF）

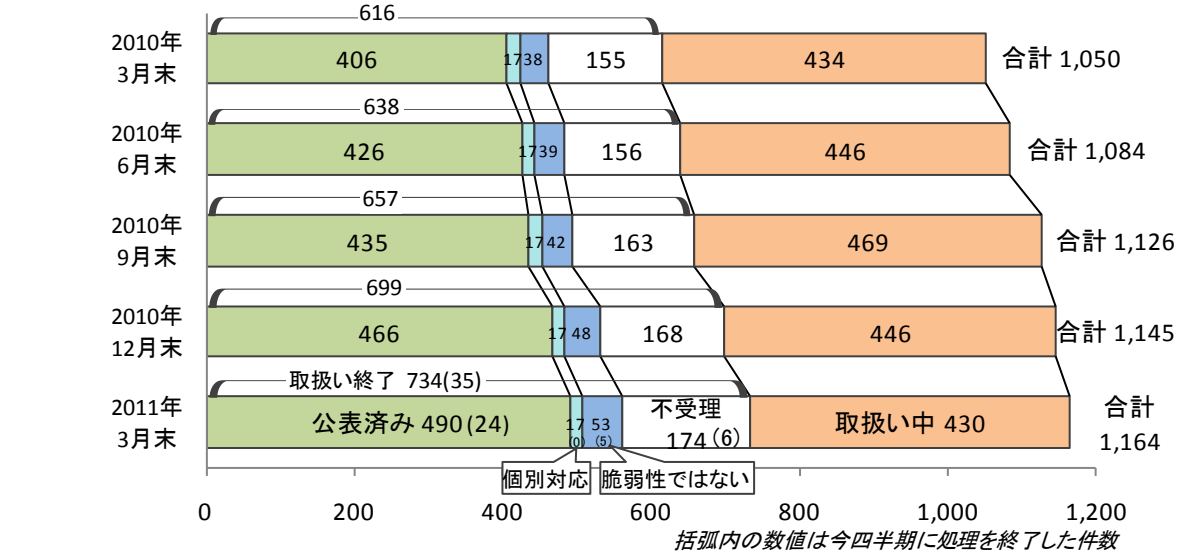
別紙 2

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 24 件（累計 490 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 5 件（累計 53 件）、「不受理」としたものは 6 件 (*1)（累計 174 件）、取扱い中は 430 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

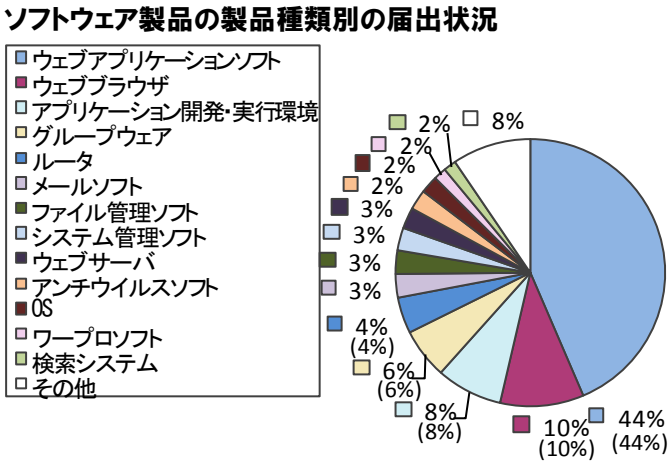
図 1-1.ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

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 1,164 件のうち、不受理を除いた 990 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。

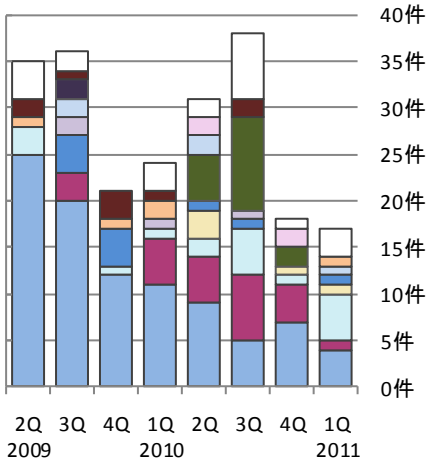
脆弱性の種類は、CMS（Contents Management System）や掲示板ソフトなどの「ウェブアプリケーションソフト」に関するものが最多となっています。また、今四半期は「アプリケーション開発・実行環境」が多くなっています。これはウェブアプリケーションサーバソフトウェアなどが多く届出されたためです。

(*1) 今四半期の届出で不受理とした 2 件、前四半期までの届出の中で今四半期に不受理とした 4 件の合計です。



※その他には、周辺機器、データベース、携帯機器などがあります。
（990件の内訳、グラフの括弧内は前四半期までの数字）

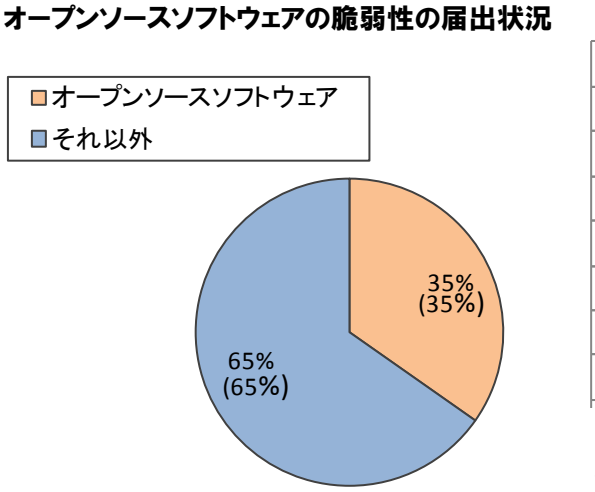
図1-2. 製品種類別の届出件数の割合



（過去2年間の届出内訳）

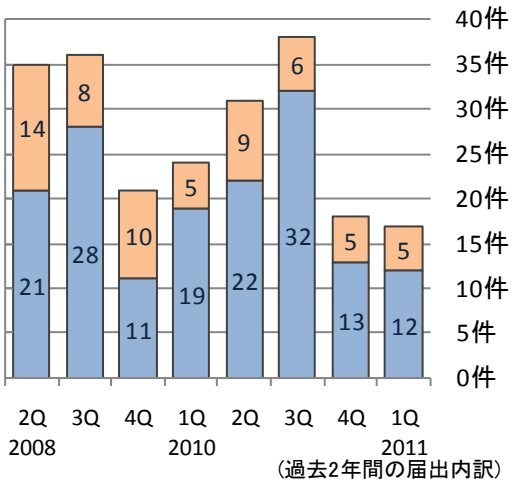
図1-3. 製品種類別の届出件数（四半期別推移）

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 1,164 件のうち、不受理のものを除いた 990 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。オープンソースソフトウェアは約 4 割あります。また、今四半期はオープンソースソフトウェアの届出が 5 件ありました。



（990件の内訳、グラフの括弧内は前四半期までの数字）

図1-4. オープンソースソフトウェアの届出件数の割合



（過去2年間の届出内訳）

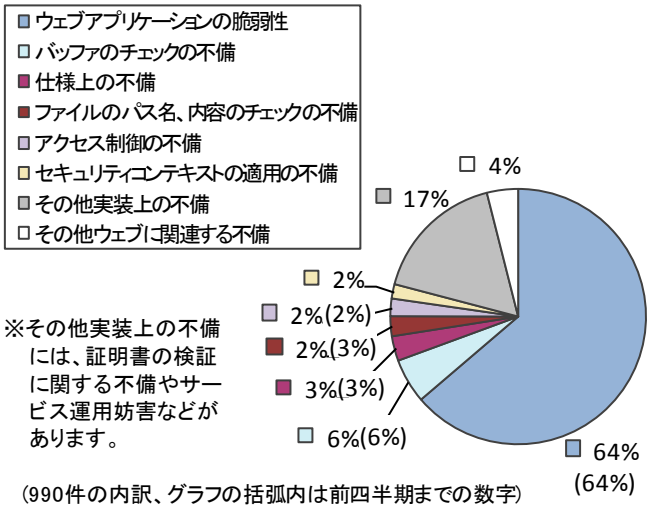
図1-5. オープンソースソフトウェアの届出件数（四半期別推移）

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 1,164 件のうち、不受理のものを除いた 990 件について、図 1-6 のグラフは原因別[*2]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」の割合が増加しています。

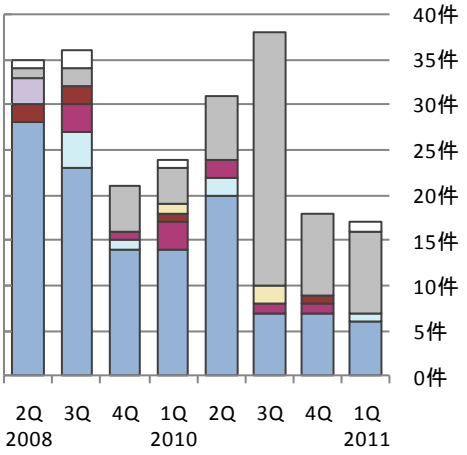
[*2] それぞれの詳しい脆弱性の原因の説明については付表 1 を参照してください。

ソフトウェア製品の脆弱性の原因別の届出状況



(990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

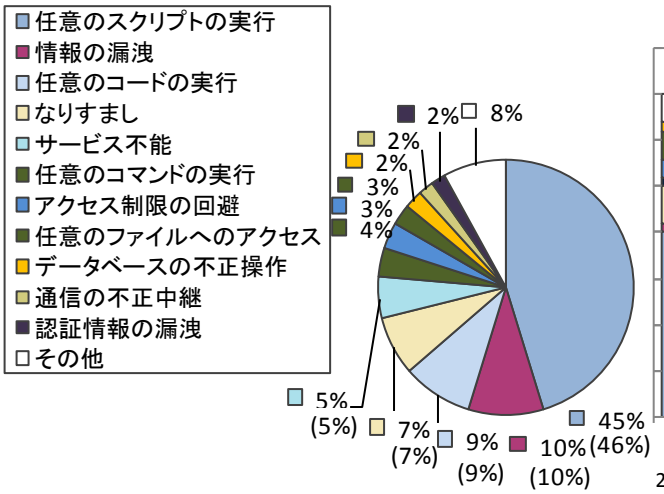


(過去2年間の届出内訳)

図1-7. 脆弱性の原因別の届出件数(四半期別推移)

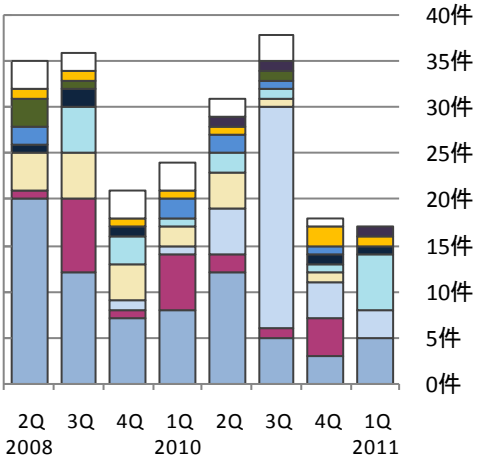
図 1-8 のグラフは脆弱性の脅威別の届出件数の割合を、図 1-9 は過去 2 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。脆弱性の脅威は「任意のスクリプト実行」が半数近くを占めています。また、今四半期から「サービス不能」が多くなっています。

ソフトウェア製品の脆弱性の脅威別の届出状況



(990件の内訳、グラフの括弧内は前四半期までの数字)

図1-8. 脆弱性の脅威別の届出件数の割合



(過去2年間の届出内訳)

図1-9. 脆弱性の脅威別の届出件数(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等の関係者との調整、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[(*3)]。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 1,105 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。

(*3) JPCERT/CC 活動概要 Page14~19（https://www.jpcert.or.jp/pr/2011/PR20110412.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	24 件	490 件
②	海外 CSIRT 等と連携して公表したもの	44 件	615 件
	合計	68 件	1,105 件

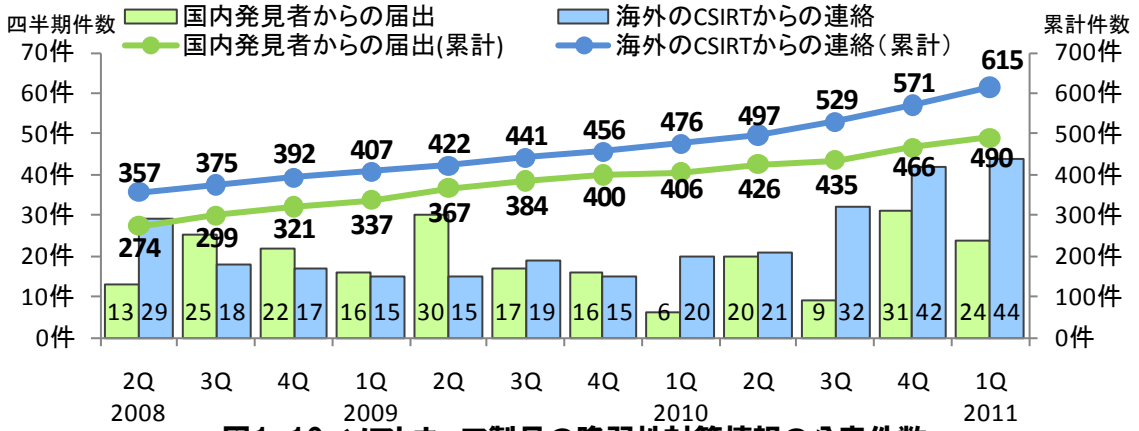


図1-10. ソフトウェア製品の脆弱性対策情報の公表件数

（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 は受理してから対応状況を JVN 公表するまでに要した日数を示したものです。45 日以内に公表された件数は 2011 年第 1 四半期で 38%になり、徐々に割合が増えていますが、公表までに 45 日を経過する届出が 62%という状況です。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。

表 1-2. 45 日以内の公表件数の四半期別推移

2008 2Q	3Q	4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q
32%	34%	34%	33%	34%	35%	35%	35%	36%	36%	38%	38%

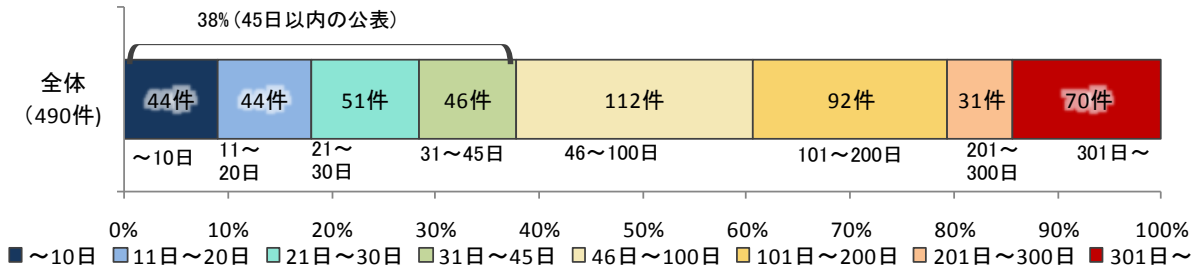


図1-11. ソフトウェア製品の脆弱性公表日数

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 7 件（表 1-3 の*1）、製品開発者自身から届けられた自社製品の脆弱性が 5 件（表 1-3 の*2）、組込みソフトウェア製品の脆弱性が 2 件（表 1-3 の*3）ありました。

表 1-3. 2011 年第 1 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 (*3)	「Cisco Linksys WRT54GC」におけるバッファオーバーフローの脆弱性	ルータ製品「Cisco Linksys WRT54GC」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、第三者によりにより応答不能にされる可能性がありました。	2011 年 1 月 21 日	7.8
2 (*1)	「MODx Evolution」における SQL インジェクションの脆弱性	コンテンツ管理システム「MODx Evolution」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、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 1 月 26 日	7.5
3 (*2) (*3)	「SEIL シリーズ」におけるバッファオーバーフローの脆弱性	ルータ製品「SEIL シリーズ」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、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 2 月 28 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)	「SquirrelMail」におけるクロスサイト・スクリプティングの脆弱性	ウェブメール「SquirrelMail」には、ウェブページを出力する際の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。	2011 年 1 月 7 日	4.3
5 (*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、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 1 月 11 日	4.0
6	「SGX-SP Final」および「SGX-SP Final NE」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「SGX-SP Final」および「SGX-SP Final NE」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。	2011 年 1 月 11 日	4.3
7	「Ruby Version Manager」におけるエスケープシーケンスインジェクションの脆弱性	Ruby 環境管理ツール「Ruby Version Manager」には、エスケープシーケンスインジェクションの脆弱性がありました。このため、端末エミュレータ等の画面に任意のエスケープシーケンスが混入する可能性がありました。	2011 年 1 月 18 日	4.3
8	複数の Rocomotion 製品におけるクロスサイト・スクリプティングの脆弱性	Rocomotion が提供する電子掲示板ソフトウェア「Pboard」などの複数の製品には、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。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 1 月 18 日	5.0
9	「Lunascape」における DLL 読み込みに関する脆弱性	ウェブブラウザ「Lunascape」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 1 月 21 日	6.8
10 (*1)	「MODx Evolution」におけるディレクトリ・トラバーサルの脆弱性	コンテンツ管理システム「MODx Evolution」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、遠隔の第三者により当該製品が設置されているサーバ内のファイルが閲覧される可能性がありました。	2011 年 1 月 26 日	5.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
11 (*1)	「EC-CUBE」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」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。	2011 年 2 月 2 日	4.3
12	「Opera」における実行ファイル読み込みに関する脆弱性	ウェブブラウザ「Opera」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 2 月 2 日	5.1
13	「F-Secure アンチウイルス Linux ゲートウェイ」における認証不備の脆弱性	ネットワーク上に設置するアンチウイルス製品「F-Secure アンチウイルス Linux ゲートウェイ」には、認証不備の脆弱性が存在しました。このため、第三者によって、当該製品に保存されているログ情報などが閲覧される可能性がありました。	2011 年 2 月 16 日	5.0
14	「Lunascape」における実行ファイル読み込みに関する脆弱性	ウェブブラウザ「Lunascape」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 2 月 23 日	5.1
15	複数のシングス CGI 製品におけるクロスサイト・スクリプティングの脆弱性	シングス が提供する「掲示板『BBS』」および「スレッド掲示板『BBS Thread』」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。	2011 年 3 月 2 日	4.3
16 (*2)	IBM「DB2」におけるサービス運用妨害 (DoS) の脆弱性	データベースソフト「DB2」には、Java Runtime Environment (JRE) の問題に起因するサービス運用妨害 (DoS) の脆弱性がありました。このため、ストアード・プロシージャーの作成および実行特権を持つユーザによりサービス運用妨害 (DoS) 状態にされる可能性がありました。	2011 年 3 月 4 日	4.0
17 (*2)	IBM「WebSphere Application Server」におけるサービス運用妨害 (DoS) の脆弱性	アプリケーションサーバー「WebSphere Application Server」には、Java Runtime Environment (JRE) の問題に起因するサービス運用妨害 (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 3 月 4 日	5.0
18 (*2)	IBM「Lotus」におけるサービス運用妨害 (DoS) の脆弱性	グループウェア「Lotus」のソフトウェア群には、Java Runtime Environment (JRE) の問題に起因するサービス運用妨害 (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 3 月 4 日	5.0
19 (*1)	「OTRS」における OS コマンド・インジェクションの脆弱性	チケット管理ソフトウェア「OTRS」には、OS コマンド・インジェクションの脆弱性がありました。このため、「OTRS」を設置しているサーバ上で、「OTRS」の実行権限で任意の OS コマンドを実行される可能性がありました。	2011 年 3 月 7 日	6.8
20 (*2)	IBM「Tivoli」製品におけるサービス運用妨害 (DoS) の脆弱性	システム管理用ソフトウェア「Tivoli」製品には、Java Runtime Environment (JRE) の問題に起因するサービス運用妨害 (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 3 月 10 日	5.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
21	「e107」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「e107」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。	2011 年 3 月 14 日	4.3
22	「Picasa」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「Picasa」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 3 月 25 日	5.1
脆弱性の深刻度=レベルⅠ（注意）、CVSS 基本値=0.0～3.9				
23 (*1)	「SquirrelMail」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「SquirrelMail」には、クロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、当該製品にログインした状態で、悪意あるページを読み込んだ場合、意図せずメールを送信されてしまうなどの可能性がありました。	2011 年 1 月 7 日	2.6
24	「Contents-Mall」におけるパスワードの取扱いに関する脆弱性	ショッピングサイト構築ソフト「Contents-Mall」には、パスワードの取扱いに関連する脆弱性がありました。このため、第三者に管理者のパスワードが漏えいし、当該製品で管理している情報を閲覧されたり、改ざんされたりする可能性がありました。	2011 年 1 月 11 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けられた自社製品の脆弱性
（*3）：組込みソフトウェアの脆弱性

（2）海外 CSIRT 等と連携して公表した脆弱性

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 41 件、表 1-5 には対応に緊急を要する Technical Cyber Security Alert の 3 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 (*4) 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	Microsoft Windows にバッファオーバーフローの脆弱性	緊急案件として掲載
2	Microsoft Internet Explorer 8 における解放済みメモリを使用する脆弱性	緊急案件として掲載
3	Apple Mac OS X 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
4	PolyVision RoomWizard に脆弱性	注意喚起として掲載
5	Ecava IntegraXor におけるディレクトリトラバーサルの脆弱性	注意喚起として掲載
6	libpng 1.5.0 の png_set_rgb_to_gray() 関数に脆弱性	注意喚起として掲載
7	Advantech Studio Test Web Server 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
8	WellinTech KingView 6.53 にヒープオーバーフローの脆弱性	緊急案件として掲載
9	Google Chrome における複数の脆弱性	注意喚起として掲載
10	ICQ 7 のアップデートに検証不備の問題	注意喚起として掲載

(*4) 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
11	Objectivity/DB 管理用ツールに認証不備の問題	注意喚起として掲載
12	CollabNet ScrumWorks Basic Server における認証情報取り扱いに関する問題	注意喚起として掲載
13	Lomtec ActiveWeb Professional 3.0 CMS における任意のファイルをアップロードおよび実行可能な脆弱性	注意喚起として掲載
14	ISC DHCPv6 にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
15	Microsoft Windows にスクリプトインジェクションの脆弱性	緊急案件として掲載
16	Cisco Tandberg E, EX および C Series における root アカウントのデフォルト認証情報の問題	注意喚起として掲載
17	Automated Solutions Modbus/TCP Master OPC Server 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
18	Sielco Sistemi Winlog 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	MOXA Device Manager MDM Tool 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
20	SCADA Engine BACnet OPC Client 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
21	IntelliCom NetBiter NB100 および NB200 プラットフォームに複数の脆弱性	注意喚起として掲載
22	Majordomo 2 におけるディレクトリトラバーサルの脆弱性	注意喚起として掲載
23	Adobe Flash に脆弱性	注意喚起として掲載
24	Adobe Shockwave Player に複数の脆弱性	注意喚起として掲載
25	Microsoft Windows にバッファオーバーフローの脆弱性	緊急案件として通知
26	PivotX において第三者にパスワードを変更される脆弱性	注意喚起として掲載
27	ISC BIND にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
28	Mutare Software Enabled VoiceMail (EVM) のウェブインターフェースに複数の脆弱性	注意喚起として掲載
29	IBM WebSphere Portal Server の入力値検証に脆弱性	注意喚起として掲載
30	Wireshark にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
31	Apple iTunes 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
32	複数の STARTTLS 実装に脆弱性	複数製品開発者へ通知
33	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
34	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
35	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
36	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
37	Adobe Flash に脆弱性	緊急案件として通知
38	MIT Kerberos 5 KDC に double free の脆弱性	注意喚起として掲載
39	Foolabs Xpdf にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
40	OpenSLP にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
41	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

表 1-5.米国 US-CERT (*5) 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	Microsoft 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

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

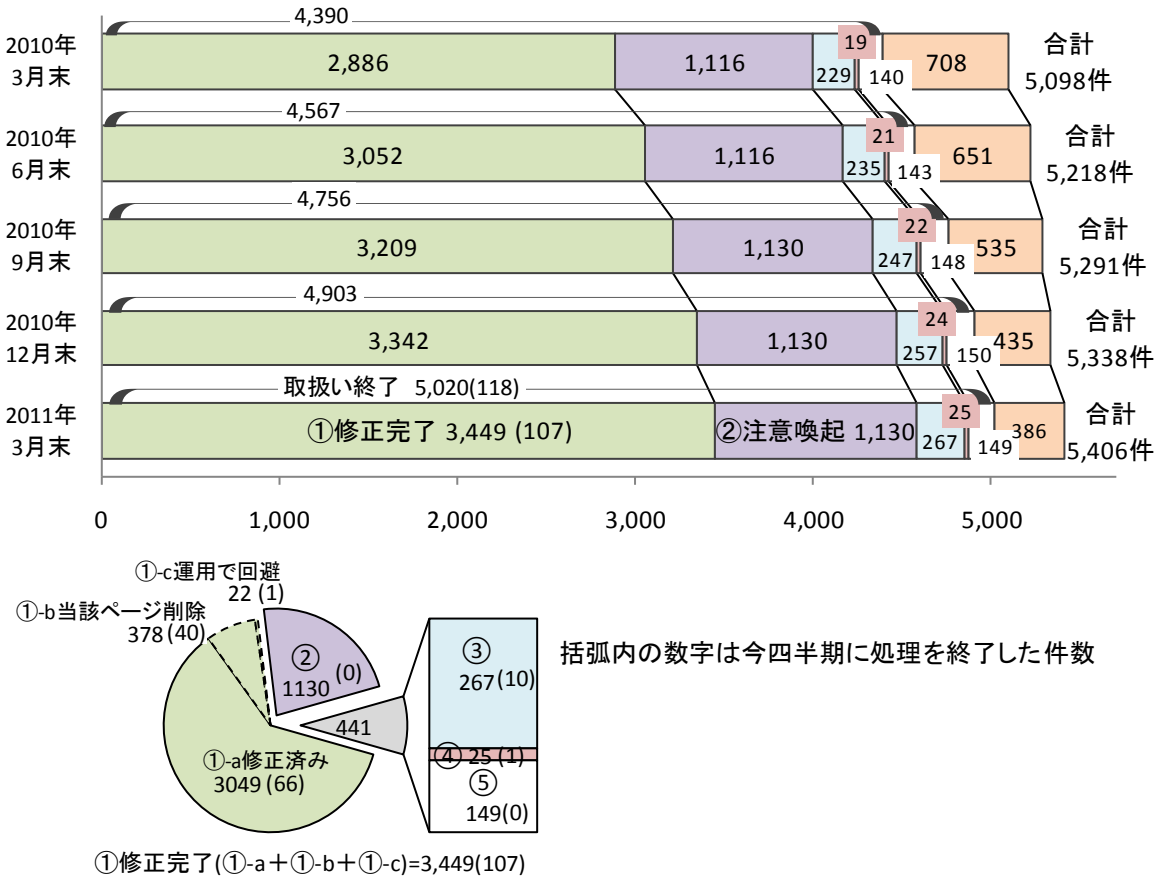
2. ウェブサイトの脆弱性の処理状況の詳細

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 118 件（累計 5,020 件）でした。このうち、「修正完了」したものは 107 件（累計 3,449 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」で広く対策を促した後、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 267 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 1 件（累計 25 件）です。「不受理」としたものは 0 件（累計 149 件）でした。

取扱いを終了した累計 5,020 件のうち、「注意喚起」「連絡不可能」「不受理」を除く累計 3,716 件（74%）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 40 件（累計 378 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 22 件）でした。



括弧内の数字は今四半期に処理を終了した件数

①修正完了(①-a＋①-b＋①-c)=3,449(107)

2011年3月末 取扱い終了の内訳

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
-a 修正済み	：	修正完了のうち、修正されたと判断したもの
-b 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
-c 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、そのうち「企業（株式・非上場）」の割合が前四半期と比較して増加しています。

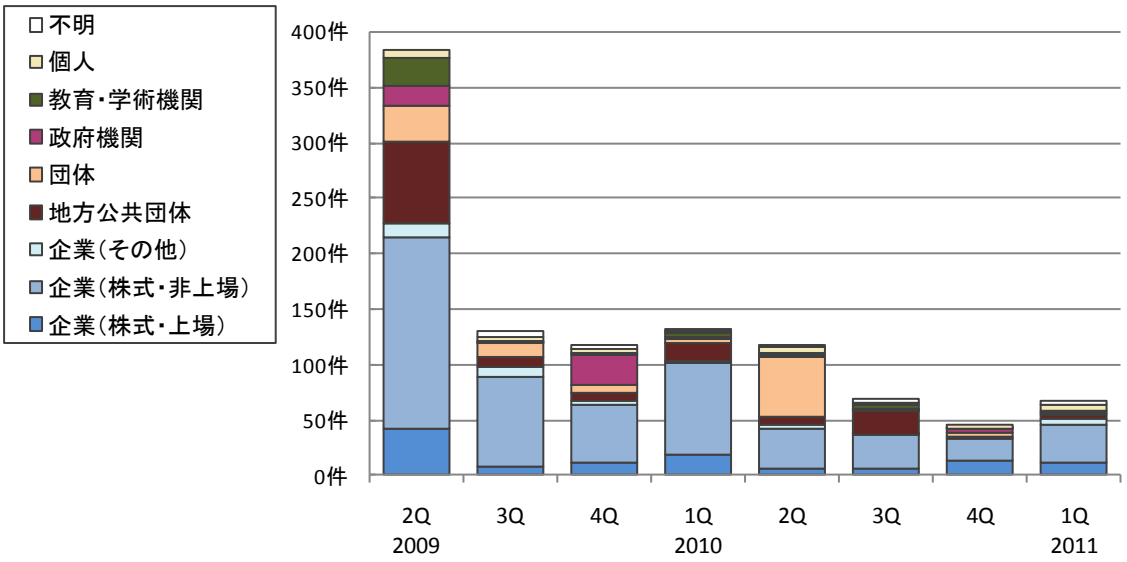
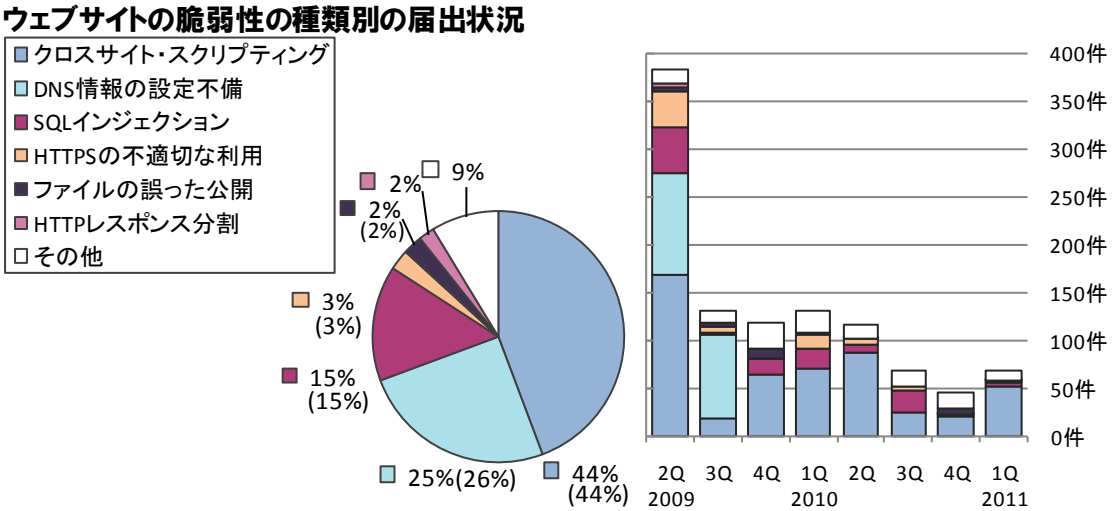


図2-2. ウェブサイトの運営主体の種類別の届出件数（四半期別推移）

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 5,406 件のうち、不受理のものを除いた 5,257 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 [*6]。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。



（5,257件の内訳、グラフの括弧内は前四半期までの数字）

（過去2年間の届出内訳）

図2-3. 脆弱性の種類別の届出件数の割合　**図2-4. 脆弱性の種類別の届出件数（四半期別推移）**

[*6] 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 のグラフは脆弱性の脅威別の届出件数の割合を、図 2-6 は過去 2 年間の脆弱性の脅威別届出件数の四半期別推移を示したものです。脆弱性の脅威は「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」「Cookie 情報の漏洩」が全体の 85%を占めています。

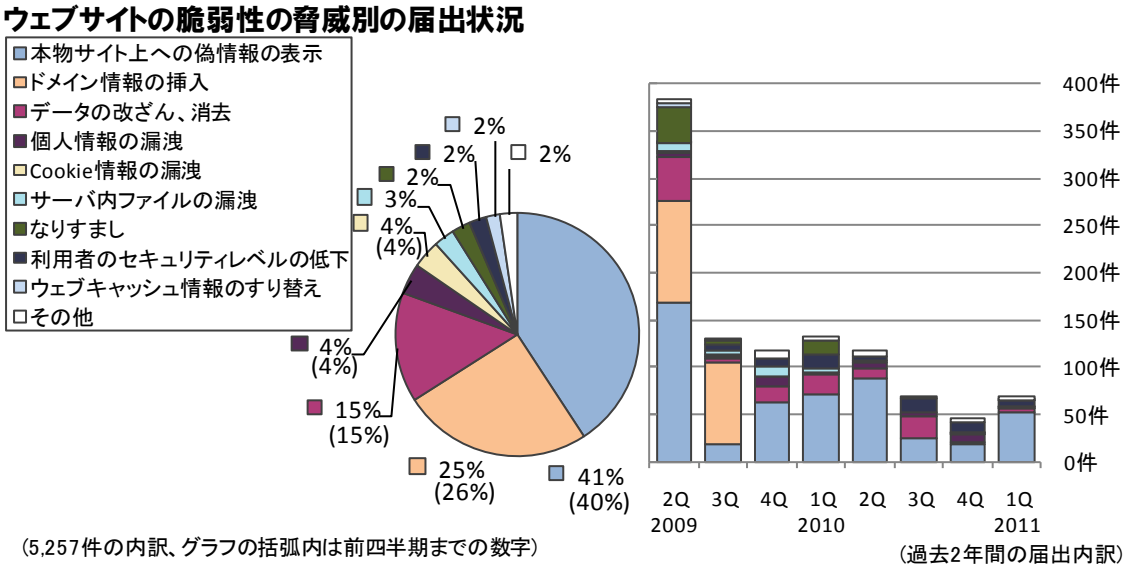


図2-5. 脆弱性の脅威別の届出件数の割合　図2-6. 脆弱性の脅威別の届出件数(四半期別推移)

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、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 日以内に修正完了となった件数の割合を示したものです。2009 年第 3 四半期以降は、90 日以内に修正完了となった割合が減少しています。

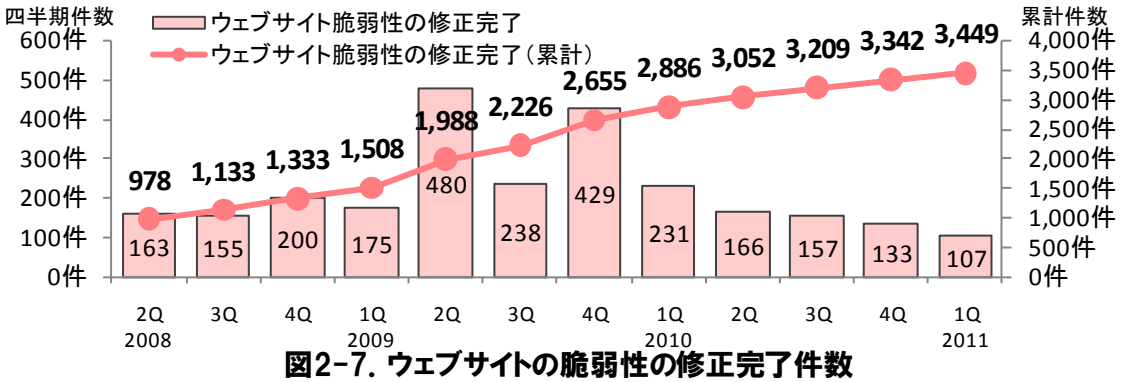


図2-7. ウェブサイトの脆弱性の修正完了件数

表 2-1. 90 日以内に修正完了した件数の四半期別割合

2008 2Q	3Q	4Q	2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q
81%	80%	83%	80%	79%	79%	72%	70%	68%	67%	66%	65%

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 [*7]。全体の 46%の届出が 30 日以内、全体の 65%の届出が 90 日以内に修正されています。

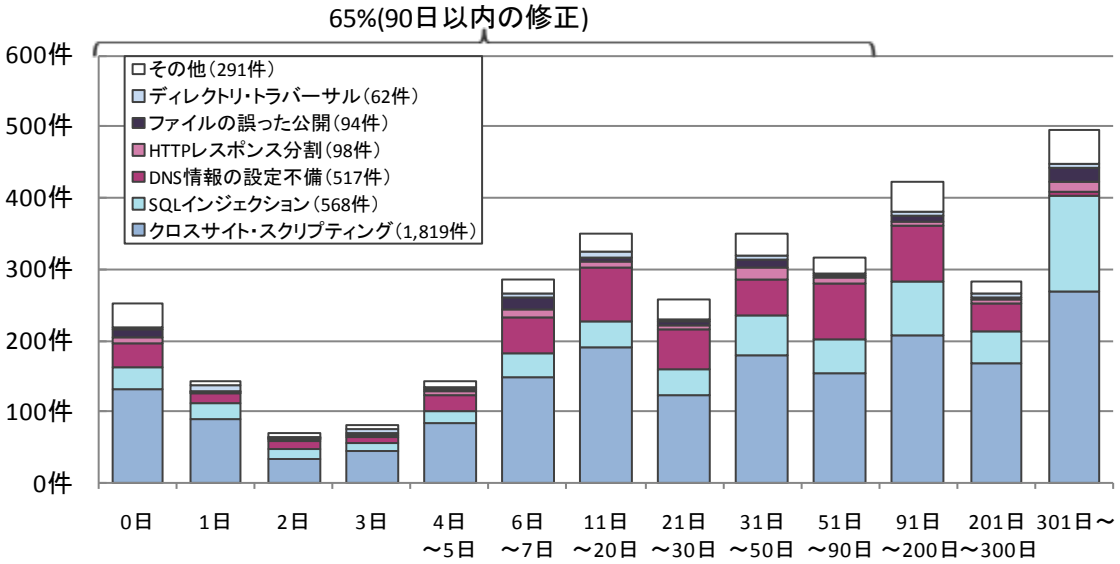


図2-8.ウェブサイトの修正に要した日数

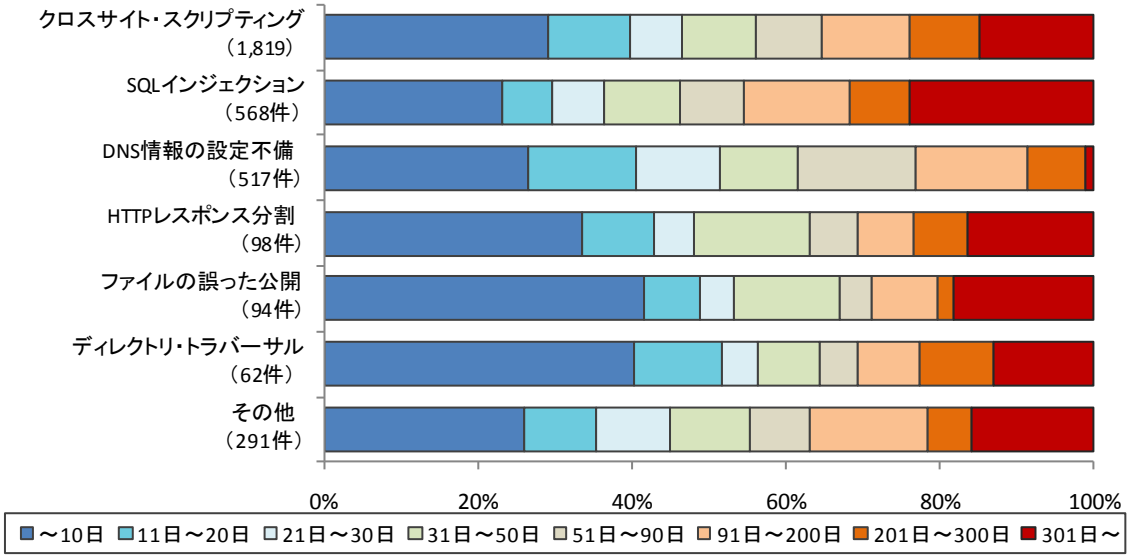


図2-9.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*7] 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など、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 18 件、200 日から 299 日のものは 20 件など、これらの合計は 309 件（前四半期は 359 件）です。前四半期の 359 件のうち、今四半期に 68 件が取扱い終了となった一方、新たに 18 件が 90 日以上経過し加わったため、合計で前四半期から 50 件の減少となりました。

表 2-2 は、四半期末の時点で取扱中の届出のうち、長期化している届出件数の四半期別推移を示しています。2009 年の第４四半期以降は、長期化している届出件数が減少傾向となっています。

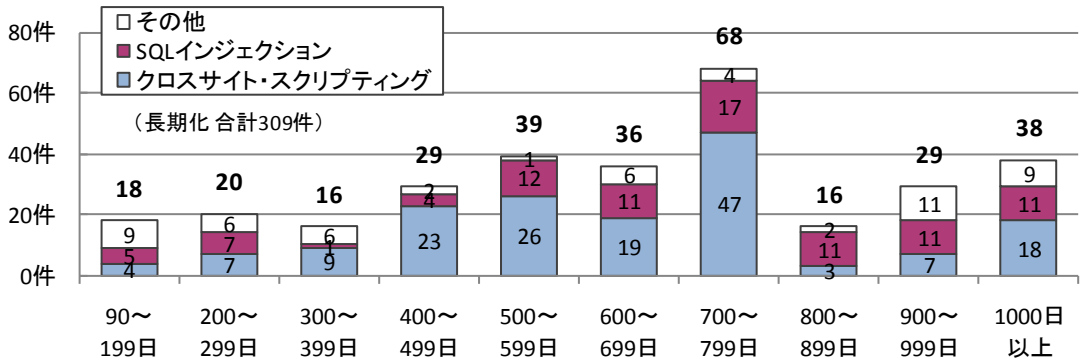


図2-10.取扱いが長期化（90日以上経過）しているウェブサイトの経過日数と脆弱性の種類

表 2-2. 取扱いが長期化している届出件数の四半期別推移

2009 1Q	2Q	3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1 Q
592 件	1,021 件	1,125 件	551 件	507 件	440 件	394 件	359 件	309 件

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

（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、以下のコンテンツもご活用ください。

「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

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ので、ご活用ください。

（4）発見者

脆弱性関連情報の適切な流通のため、届出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

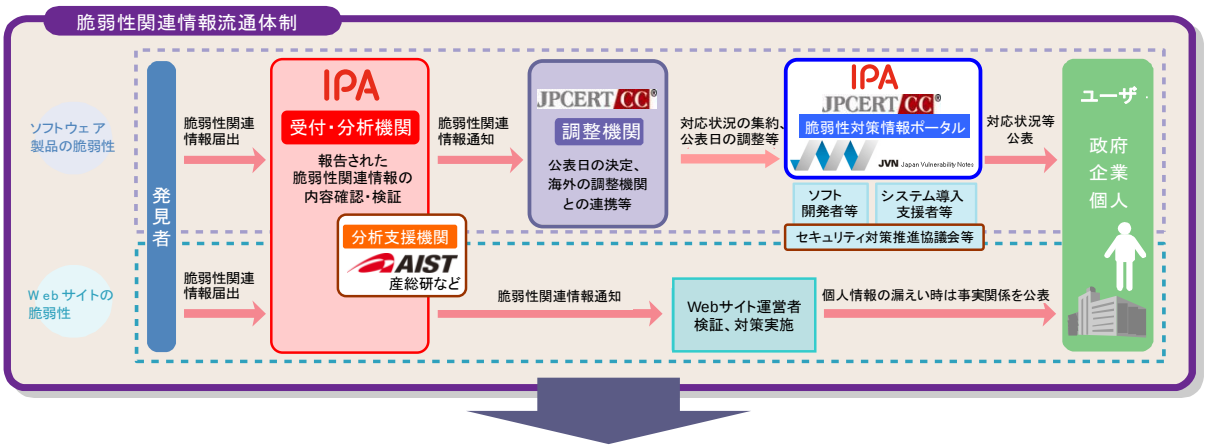
付表 2 ウェブサイト脆弱性の分類

	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