プレスリリース
2010 年 4 月 27 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 [2010 年第 1 四半期（1 月～3 月）]

～ 2009 年度に届出られた携帯サイトの脆弱性の 1/3 以上が「なりすましの危険性あり」 ～

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）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、2010 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) 2009 年度に届出られた携帯サイトの脆弱性の 1/3 以上が「なりすましの危険性あり」

IPA には、パソコン向けのウェブサイトの脆弱性だけでなく、携帯電話向けのウェブサイト（以降、携帯サイト）に関する脆弱性も届出られています。届出られた脆弱性に関して携帯サイトの脆弱性には、「セッション管理の不備」や「認証に関する不備」といった、他人になりすますことが可能となる脆弱性が多いという特徴があります。2009 年度に届出られた脆弱性のうち、そのような脆弱性の占める割合は、ウェブサイト（携帯サイトを含む届出全体）の場合が 4%であるのに対し、携帯サイトの場合は 37%を占めています。

このように、携帯サイトに関しても深刻な脆弱性があることから、その運用にあたってはパソコン向けウェブサイトと同様に十分な脆弱性対策が求められます。

(2) ウェブサイトの脆弱性の届出件数の累計が 5,000 件を突破

2010 年第 1 四半期の IPA への脆弱性関連情報の届出件数は 171 件です。内訳は、ソフトウェア製品に関するものが 32 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 139 件です。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 1,050 件、ウェブサイトに関するものが 5,098 件、合計 6,148 件となりました。

(3) 修正済み脆弱性の約半分が最近の 15 か月間で修正を完了

2004 年 7 月の届出受付開始からのソフトウェア製品およびウェブサイトの脆弱性の修正完了件数の累計は 3,309 件となりました。このうち 2009 年 1 月から 2010 年 3 月末までの 15 か月で修正を完了した件数は 1,638 件であり、これまでに修正を完了した届出案件の約半分がこの期間に完了したことになります。これは 2008 年第 4 四半期から 2009 年第 1 四半期に掛けて、届出件数が増加したことにより取扱件数が増え、その結果、修正完了件数が増加したことが主な要因と考えられます。

これらの事象から、本届出制度が着実に浸透してきていると考えられます。

■ 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] ソフトウェア等の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

1. 2010 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）

1.1 脆弱性関連情報の届出状況

～ウェブサイトの脆弱性の届出件数の累計が 5,000 件を突破～

2010 年第 1 四半期の IPA への脆弱性関連情報の届出件数は、ソフトウェア製品に関するもの 32 件、ウェブアプリケーション（ウェブサイト）に関するもの 139 件、合計 171 件でした（表 1）。

表 1. 2010 年第 1 四半期の届出件数

分類	届出件数	累計件数
ソフトウェア製品	**32** 件	**1,050** 件
ウェブサイト	**139** 件	**5,098** 件
合計	**171** 件	**6,148** 件

届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 1,050 件、ウェブサイトに関するもの 5,098 件、合計 6,148 件となりました（表 1）。ウェブサイトに関する届出が全体の 83%を占めています。ウェブサイトに関する届出は 2009 年第 3 四半期から 130 件前後で推移しています（図 1）。1 就業日あたりの届出件数は 2010 年第 1 四半期末で 4.40 件となりました（表 2）。

表 2. 届出件数（2004 年 7 月 8 日の届出受付開始から各四半期末時点）

	2007 1Q	2008 1Q	2Q	3Q	4Q	2009 1Q	2Q	3Q	4Q	2010 1Q
累計届出件数[件]	1,310	2,045	2,322	2,885	4,375	5,227	5,656	5,826	5,977	6,148
1就業日あたり[件/日]	1.95	2.24	2.38	2.79	4.00	4.53	4.66	4.56	4.47	4.40

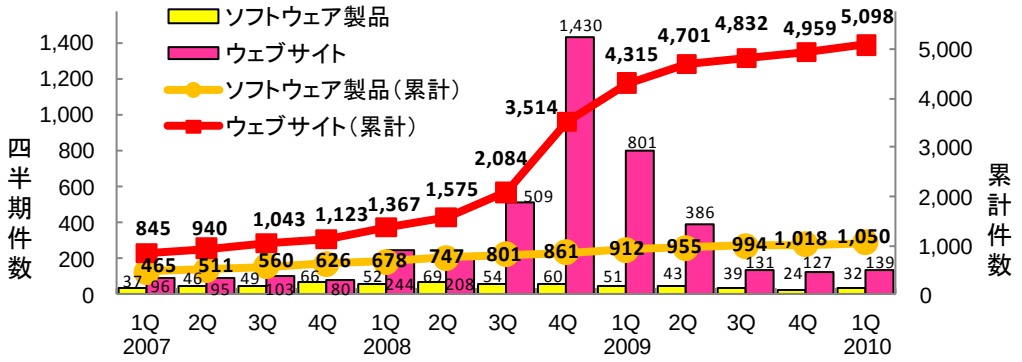


図1.脆弱性関連情報の届出件数の四半期別推移

1.2 脆弱性の修正完了状況

～ 修正済み脆弱性の約半分が最近の 15 か月間で修正を完了 ～

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、2010 年第 1 四半期に JVN[2]で対策情報を公表したものが 6 件（累計 406 件）でした。

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を行い、2010 年第 1 四半期に修正を完了したものが 232 件（累計 2,886 件）でした。

2004 年 7 月の届出受付開始から、修正完了件数の累計（ソフトウェア製品、ウェブサイト）は 3,309 件となりました。このうち、2009 年 1 月から 2010 年 3 月末までの期間に 1,638 件（修正完了件数累計の約 50%）が修正を完了しています。**四半期単位の修正完了件数は年々増加しており、本制度が着実に浸透してきています。今後も、脆弱性対策を促進する制度として広く活用されることを期待します。**

[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/

1.3 携帯サイトの脆弱性対策の実施を

2010 年第 1 四半期は、「OpenPNE」におけるアクセス制限回避の脆弱性[3]に関して、JVN で対策情報を公表しました。IPA には「OpenPNE」のように携帯サイト[4]を構築するソフトウェア製品に限らず、携帯サイトに関する脆弱性も届出られています。

携帯サイトに関する届出においては、「セッション管理の不備」および「認証に関する不備」に関する脆弱性が多く届出られています。2009 年度における携帯サイトとウェブサイト（携帯サイトを含む届出全体）の脆弱性の割合で比較すると、ウェブサイトにおける「セッション管理の不備」および「認証に関する不備」に関する届出が全体の約 4%であったのに対して携帯サイトでは約 37%でした。（図 2）。

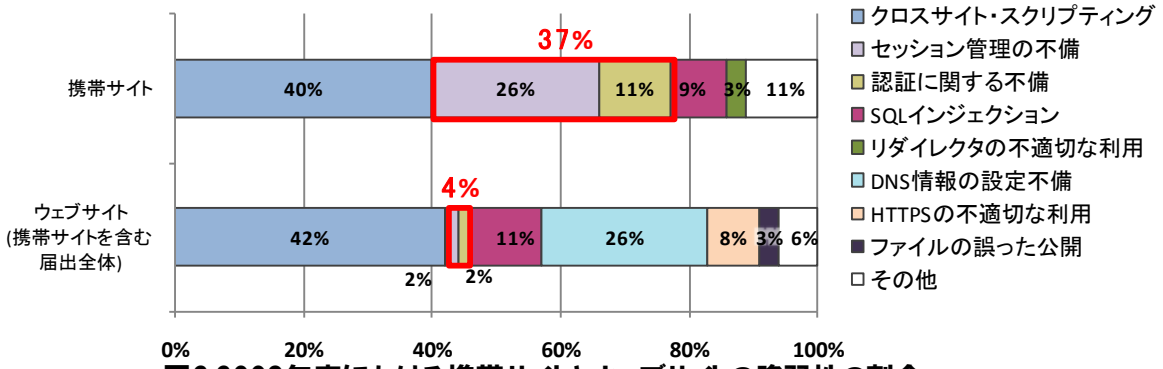


図2.2009年度における携帯サイトとウェブサイトの脆弱性の割合

携帯電話のウェブブラウザをパソコンのウェブブラウザと比べた場合、「Cookie に対応していないブラウザがある」、「閲覧しているウェブサイトのアドレスがブラウザ上に表示されない」といった違いがあります。携帯電話の高機能化等にともない、携帯サイトに脆弱性があると、その脆弱性が悪用される可能性が高まっています。

携帯サイトの運営者は、パソコン向けウェブサイトと同様に十分な脆弱性対策をお願いします。

1.4 ウェブサイト運営者は脆弱性対策の早急な実施を

ウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上ウェブサイト運営者から脆弱性を修正した旨の通知がない長期化している届出が 507 件あります。これらの届出についてウェブサイト運営主体別の件数は、企業（株式・非上場）は 266 件（52%）、地方公共団体は 84 件（17%）、その他は 57 件（11%）、企業（株式・上場）は 44 件（9%）などとなっております（図 3）。

また、長期化している届出のうち、経過日数が 400 日を超えているのは、企業（株式・上場）は 73%、企業（株式・非上場）は 61%、政府機関は 50%などとなっており、これらのウェブサイトは、１年以上脆弱性が放置されている可能性があります（図 4）。

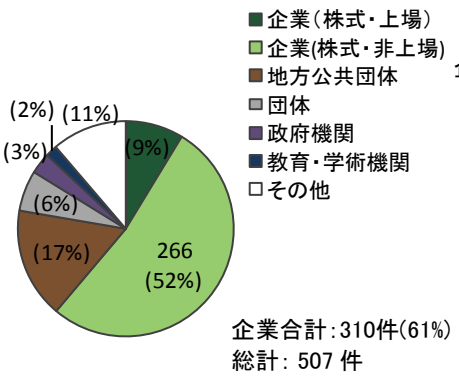


図3.取扱い中届出の運営主体別割合

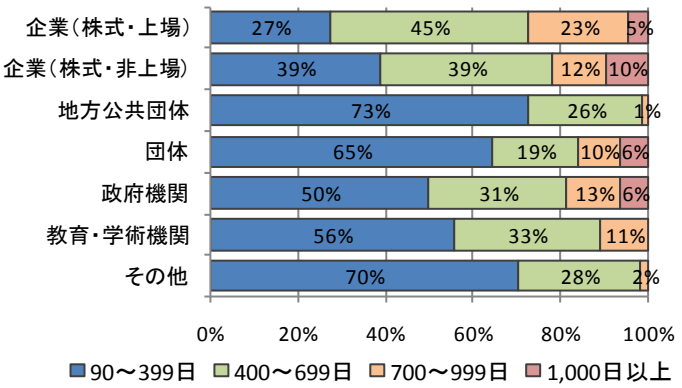


図4.取扱い長期化（90日以上）の運営主体別経過日数

[3] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=5.8、別紙 P.11 表 1-2 項番 4 を参照下さい。
[4] 「携帯電話のウェブブラウザで閲覧することを想定しているウェブサイト」を指します。

ウェブサイト運営者は長期間脆弱性が放置されることによって、脆弱性を発見され攻撃を受ける可能性が高まることを認識し、迅速に対策を講じる必要があります。早期に対策が難しい場合は、対策実施までの期間について、攻撃による影響を低減する対策[5]を実施することを推奨します。

1.5 製品開発者は「自社製品に関する脆弱性関連情報の届出」の活用を

2004 年 7 月の届出開始から、ソフトウェア製品開発者からの自社製品に関する脆弱性関連情報の届出の累計は 57 件ありました。2008 年までは届出件数が増加傾向にありましたが、2009 年は届出件数が減少しています（図 5）。

また、ソフトウェア製品に関する脆弱性関連情報の届出は、製品開発者以外は 93%、製品開発者は 7%となります（図 6）。「自社製品に関する脆弱性関連情報の届出」を活用することにより、JVN にて対策情報が公表され、より多くの利用者に対策情報を提供することが可能となります。**製品開発者は、利用者に広くソフトウェア製品の対策情報を公表するために本届出制度を有効に活用することを推奨します。**

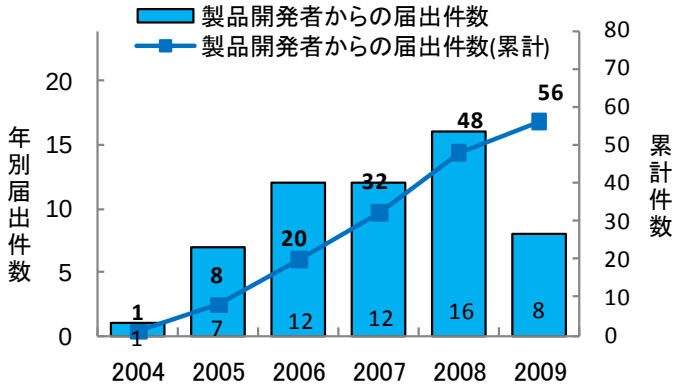


図5.製品開発者からの年別届出件数

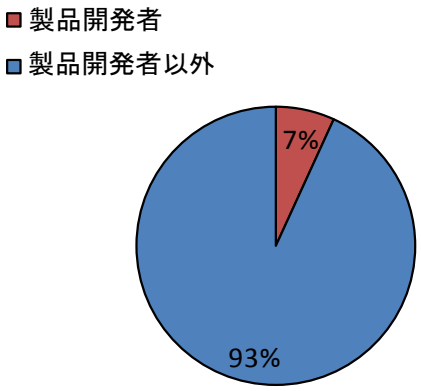


図6. 発見者の割合

[5] 「安全なウェブサイトの作り方 改訂第 4 版」を参照下さい。
http://www.ipa.go.jp/security/vuln/websecurity.html

2.ソフトウェア製品の脆弱性の処理状況

表 3. 製品の脆弱性の終了件数

分類		件数	累計
修正完了	公表済み	6 件	406 件
	個別対応	0 件	17 件
脆弱性ではない		1 件	38 件
不受理		4 件	155 件
合計		11 件	616 件

2010 年第 1 四半期のソフトウェア製品の脆弱性の処理状況は、JPCERT/CC が調整[6]を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものが 6 件（累計 406 件）、製品開発者が個別対応を行ったものは 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 38 件）、告示で定める届出の対象に該当せず不受理としたものは 4 件（累計 155 件）でした。これら取扱いを終了したものの合計は 11 件（累計 616 件）です（表 3）。

この他、海外の CSIRT[7]から JPCERT/CC が連絡を受けた 20 件（累計 476 件）を JVN で公表しました。これらの公表済み件数の期別推移を図 7 に示します。

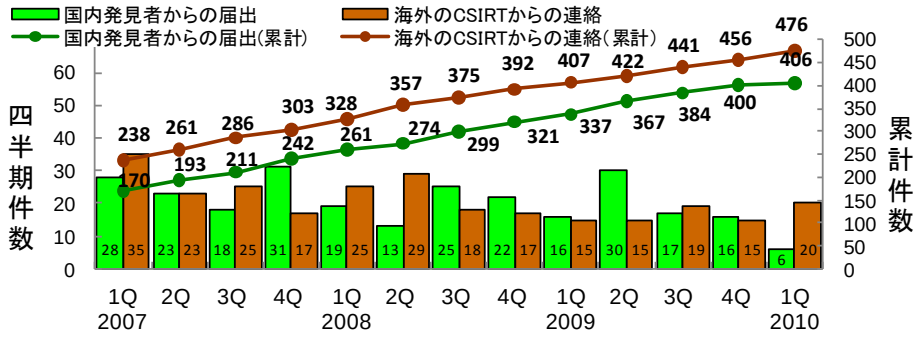


図7.ソフトウェア製品の脆弱性対策情報の公表件数

2.1 JVN で公表した主な脆弱性対策情報

今四半期は、(1)「Movable Type」におけるアクセス制限回避の脆弱性[8]、(2)「WebCalenderC3」におけるクロスサイト・スクリプティングの脆弱性[9]、(3)「WebCalenderC3」におけるディレクトリ・トラバーサルの脆弱性[10]、(4)「OpenPNE」におけるアクセス制限回避の脆弱性[11]などの脆弱性対策情報を JVN で公表しました。

3.ウェブサイトの脆弱性の処理状況

表4.ウェブサイトの脆弱性の終了件数

分類	件数	累計
修正完了	232 件	2,886 件
注意喚起	0 件	1,116 件
脆弱性ではない	12 件	229 件
連絡不可能	3 件	19 件
不受理	7 件	140 件
合計	254 件	4,390 件

2010 年第 1 四半期のウェブサイトの脆弱性の処理状況は、IPA が通知を行い、ウェブサイト運営者が修正を完了したものが 232 件（累計 2,886 件）、IPA が注意喚起等を行った後に取扱いを終了したものが 0 件（累計 1,116 件[12]）、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が 12 件（累計 229 件）、ウェブサイト運営者と連絡が不可能なものが 3 件（累計 19 件）、告示で定める届出の対象に該当せず不受理としたものが 7 件（累計 140 件）でした。

取扱いを終了したものの合計は 254 件（累計 4,390 件）です（表 4）。これらのうち、修正完了件数の期別推移を図 8 に示します。

---

[6] JPCERT/CC 活動概要 Page13~15(http://www.jpcert.or.jp/pr/2010/PR20100408.pdf)を参照下さい。
[7] Computer Security Incident Response Team。コンピュータセキュリティインシデント対応チーム。コンピュータセキュリティに関するインシデント（事故）への対応・調整・サポートをする組織です。
[8] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=5.5、別紙 P.11 表 1-2 項番 1 を参照下さい。
[9] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.3、別紙 P.11 表 1-2 項番 2 を参照下さい。
[10] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=5.0、別紙 P.11 表 1-2 項番 3 を参照下さい。
[11] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=5.8、別紙 P.11 表 1-2 項番 4 を参照下さい。
[12] 前期に注意喚起にて取扱終了し、今期に運営者から修正完了報告を受けた届出が 3 件ありました。この為、注意喚起の累計が 3 件減少し、修正完了が 3 件増加しました。

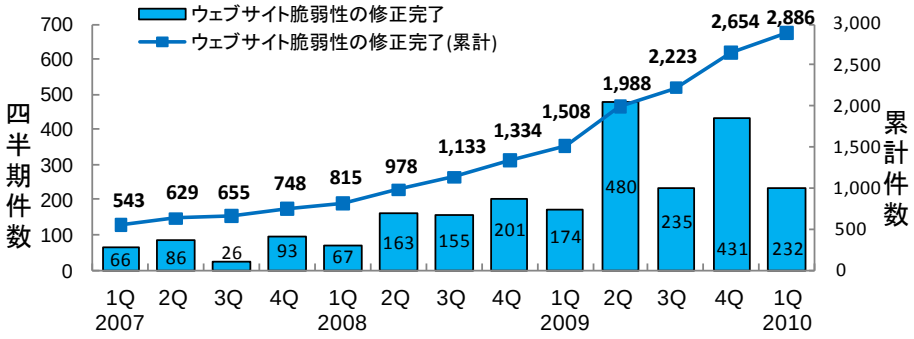


図8.ウェブサイトの脆弱性の修正完了件数

3.1 届出のあった対象ウェブサイトの運営主体の内訳と脆弱性の種類

今四半期に IPA に届出のあったウェブサイトの脆弱性関連情報 139 件のうち、不受理としたものを除いた 132 件について、対象ウェブサイトの運営主体別内訳は、企業合計が 104 件（79%）、地方公共団体が 16 件（13%）、教育・学術機関が 3 件（2%）、政府機関が 3 件（2%）、団体が 3 件（2%）などです（図 9）。

また、これらの脆弱性の種類は、クロスサイト・スクリプティングが 70 件（53%）、SQL インジェクションが 21 件（16%）、HTTPS の不適切な利用 14 件（11%）、セッション管理の不備 6 件（5%）などです（図 10）。

ウェブサイト運営者は脆弱性を作り込まないようなウェブサイトの企画・設計にあたることが必要です。届出件数が多く広く知れ渡っている脆弱性は、悪意のある第三者に発見される可能性も高く、特に注意する必要があります。

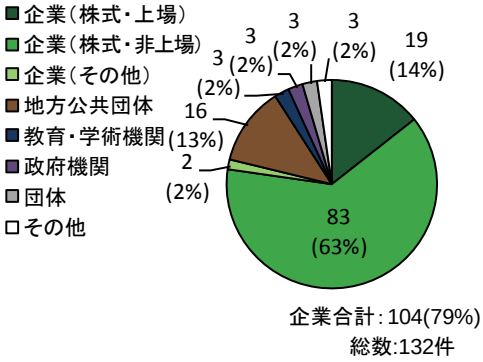


図9.ウェブサイトの運営主体（2010年1Q）

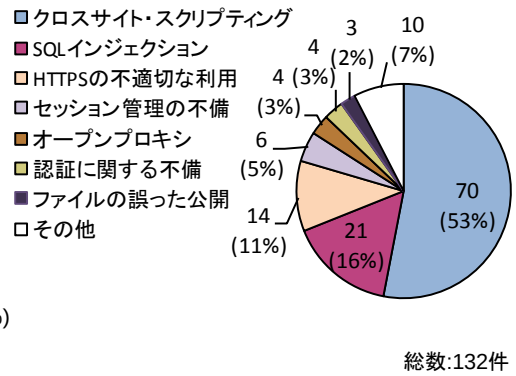


図10.ウェブサイトの脆弱性の種類（2010年1Q）

3.2 ウェブサイトの脆弱性で 90 日以上対策が未完了の届出は 507 件

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脅威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。

未修正のウェブサイトの脆弱性関連情報のうち、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までの経過日が 90 日以上経過しているものについて、経過日数毎の件数を図 11 に示します。経過日数が 90 日から 199 日に達したものは 77 件、200 日から 299 日のものは 63 件など、これらの合計は 507 件（前四半期は 551 件）です。前四半期の 551 件のうち、今四半期に 119 件が修正完了となり減少した一方、新たに 75 件が 90 日以上経過したため増加し、合計で前四半期から 44 件の減少となりました。

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。**

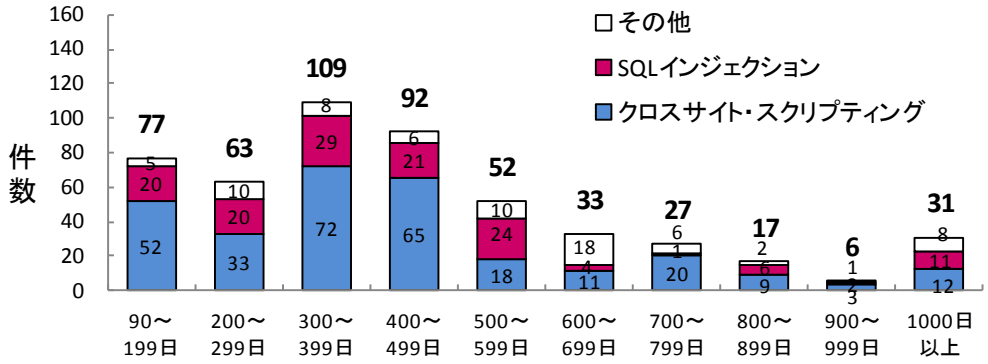


図11. 取扱いが長期化（90日以上経過）している未修正のウェブサイトの経過日数と脆弱性の種類

3.3 ウェブサイトを狙った攻撃に関する注意喚起

ウェブサイトを狙った攻撃が継続していることから、IPA は 2009 年 8 月 17 日にウェブサイト管理者等へウェブサーバのアクセスログ調査、ウェブサイトの脆弱性検査、および脆弱性対策の早急な実施を推奨する注意喚起を行いました[13]。

攻撃の現状を把握する実例として、IPA が無償で公開している「SQL インジェクション検出ツール iLogScanner[14]」で、IPA が公開している「脆弱性対策情報データベース JVN iPedia[15]」の 2009 年 1 月から 2010 年 3 月末までのアクセスログを解析した事例を示します（図 12）。注意喚起（2009 年 8 月）以降も攻撃が継続しています。

2009 年から 2010 年 3 月末までの期間で攻撃があったと思われる件数 6,692 件のうち、SQL インジェクション攻撃[16]が 3,068 件（46%）、ウェブサーバのパスワードファイルや環境設定ファイル[17]の情報を狙ったディレクトリ・トラバーサル攻撃が 2,493（37%）を占めています。ウェブサイト管理者は引き続きウェブサイトの脆弱性対策が必要です。

ウェブサイトを狙った攻撃があったと思われる件数

解析対象のウェブサイト：JVN iPedia（脆弱性対策情報データベース）
解析したウェブサーバのアクセスログの期間：2009年1月～2010年3月
攻撃があったと思われる件数：平均14.7件/日、攻撃が成功した可能性の高い件数：0件

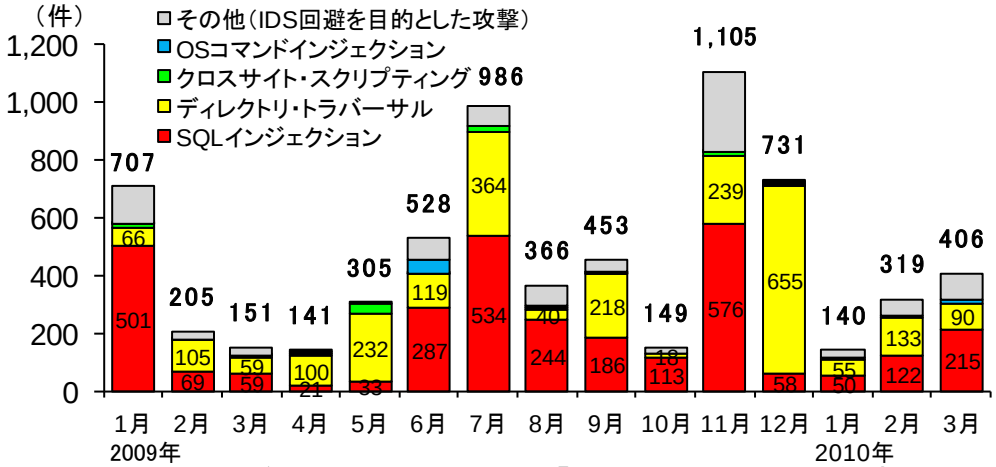


図12. SQLインジェクション検出ツール「iLogScanner」の解析事例

[13] 「ウェブサイトを狙った攻撃に関する注意喚起」を参照下さい。
http://www.ipa.go.jp/security/vuln/documents/2009/200908_attack.html
[14] ウェブサイトの脆弱性検出ツール iLogScanner。http://www.ipa.go.jp/security/vuln/iLogScanner/index.html
[15] 脆弱性対策情報データベース JVN iPedia（ジェイブイエヌ アイ・ペディア）は、国内で利用されているソフトウェアを対象にした脆弱性対策情報を網羅・蓄積し、公開しています。http://jvndb.jvn.jp/
[16] 2008 年 5 月 15 日に発行した「SQL インジェクション攻撃に関する注意喚起」を参照下さい。
http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html
[17] 具体的には、passwd ファイル、environ ファイル、resolv.con ファイルなど。

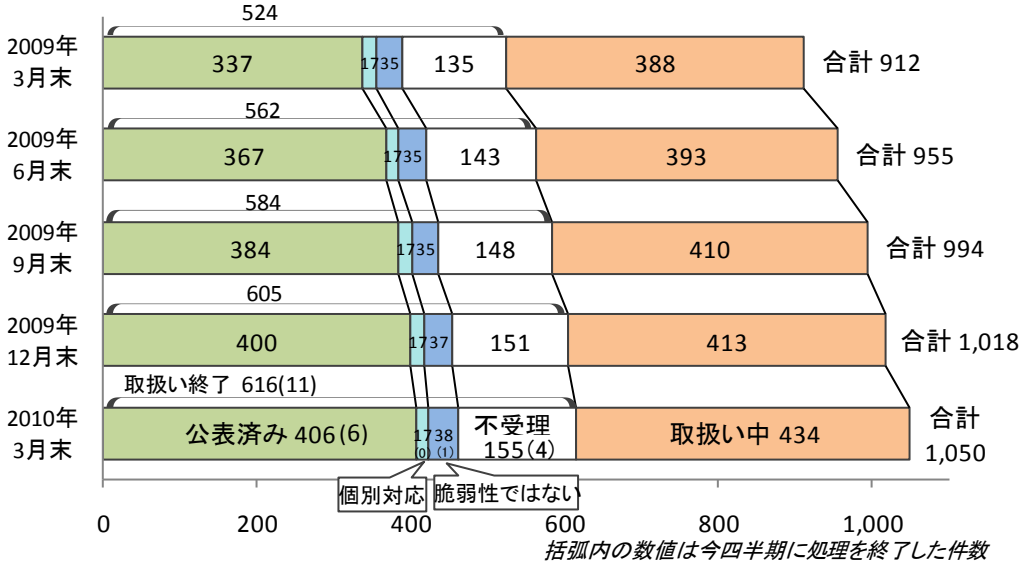
別紙 2

届出のあった脆弱性の処理状況の詳細

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

ソフトウェア製品の脆弱性関連情報の届出について、処理状況を図 1-1 に示します。今四半期に公表した脆弱性は 6 件（累計 406 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 38 件）、「不受理」としたものは 4 件（累計 155 件）、取扱い中は 434 件です。



括弧内の数値は今四半期に処理を終了した件数

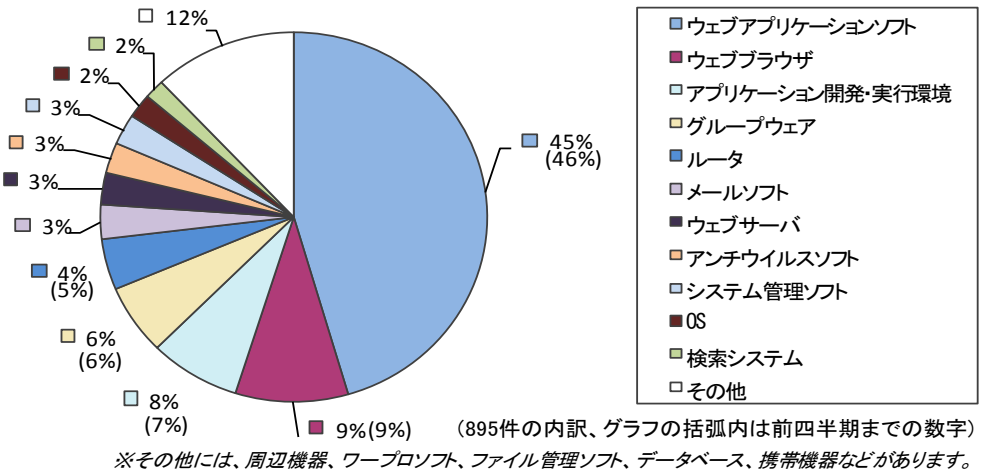
公表済み	：JVN で脆弱性への対応状況を公表したもの
個別対応	：製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない	：製品開発者により脆弱性ではないと判断されたもの
不受理	：告示で定める届出の対象に該当しないもの
取扱い中	：製品開発者が調査、対応中のもの

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 1,050 件のうち、不受理のものを除いた 895 件の製品種類別の内訳を図 1-2 に示します。

図 1-2 に示すように、IPA に届出のあった脆弱性には、「ウェブアプリケーションソフト」に関するものが多くあります。



（895件の内訳、グラフの括弧内は前四半期までの数字）

※その他には、周辺機器、ワープロソフト、ファイル管理ソフト、データベース、携帯機器などがあります。

図1-2.ソフトウェア製品の脆弱性 製品種類別内訳（届出受付開始から2010年3月末まで）

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 1,050 件のうち、不受理のものを除いた 895 件について、オープンソースソフトウェアとそれ以外のソフトウェアの脆弱性の届出件数の推移を図 1-3 に示します。今四半期はオープンソースソフトウェアの届出が 6 件ありました。2006 年頃までは上昇傾向でしたが、2008 年以降は徐々に減少しつつ推移しています。

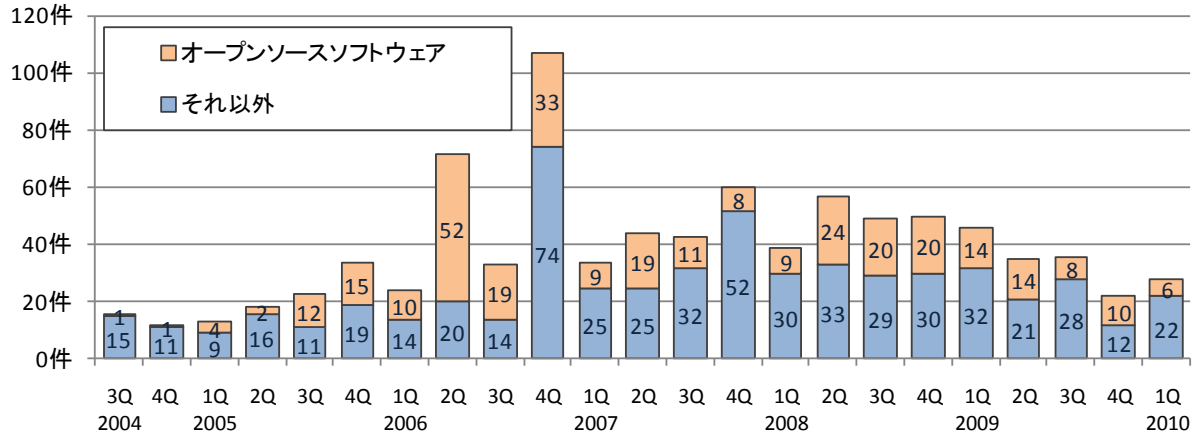
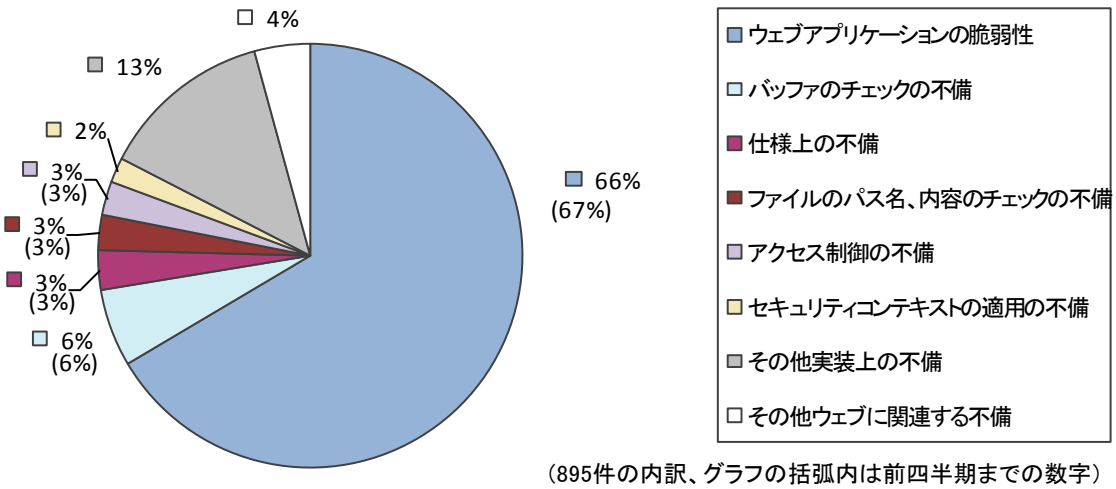


図 1-3.オープンソースソフトウェアの脆弱性の届出件数　（895件の内訳）

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 1,050 件のうち、不受理のものを除いた 895 件の原因別[18]の内訳を図 1-4 に、原因別の届出件数の推移を図 1-5 に、脅威別の内訳を図 1-6 に示します。

図 1-4 に示すように、脆弱性の原因は「ウェブアプリケーションの脆弱性」が最も多く、図 1-6 に示すように、脅威については「任意のスクリプト実行」が最も多く見られました。この傾向は図 1-5 に示すように、届出受付開始から割合を増やしつつ続いています。これは、「ウェブアプリケーションソフト」以外のソフトウェア製品でも、ウェブブラウザから管理、使用するものが多くあり、そこに脆弱性が存在する場合、比較的見つけやすいことが理由と考えられます。



（895件の内訳、グラフの括弧内は前四半期までの数字）

図 1-4.ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2010年3月末まで）

[18] 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。

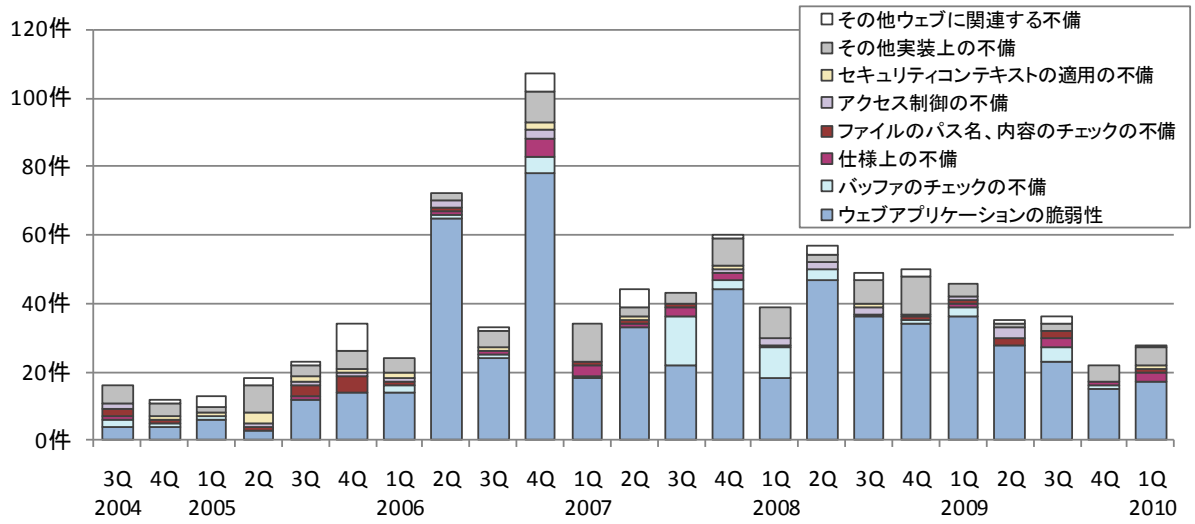
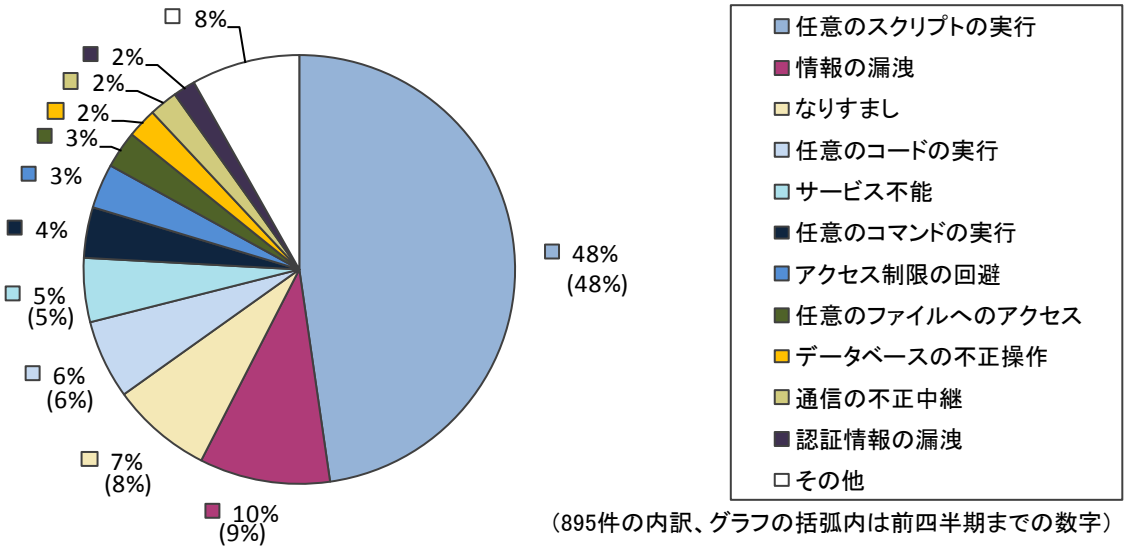


図1-5. ソフトウェア製品の脆弱性 原因別届出件数の推移（届出受付開始から2010年3月末まで）



（895件の内訳、グラフの括弧内は前四半期までの数字）

図1-6. ソフトウェア製品の脆弱性 脅威別内訳（届出受付開始から2010年3月末まで）

1.4 ソフトウェア製品の脆弱性情報の調整および公表状況

JPCERT/CC は、表 1-1 に示す 2 種類の脆弱性関連情報について、日本国内の製品開発者等の関係者との調整、および海外 CSIRT の協力のもと海外の製品開発者との調整を行っています。これらの脆弱性関連情報に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）において公表しています。（URL： http://jvn.jp/ ）

表 1-1. 脆弱性関連情報の提供元別 脆弱性公表件数

	情報提供元	今期	累計
①	国内の発見者から IPA に届出があったもの、および、製品開発者自身から自社製品の脆弱性、対策方法について届出を受けたもの	6 件	406 件
②	海外 CSIRT 等と連携して公表したもの	20 件	476 件
	合計	26 件	882 件

（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、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図 1-7 に示します。届出受付開始から各四半期末までの 45 日以内に公表される件数が 35%であり、徐々に割合が増え

ていますが、公表までに時間を要している割合が多いです。製品開発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。

45 日以内の公表件数の割合

2008/3Q まで	2008/4Q まで	2009/1Q まで	2009/2Q まで	2009/3Q まで	2009/4Q まで	2010/1Q まで
32%	32%	33%	34%	35%	35%	35%

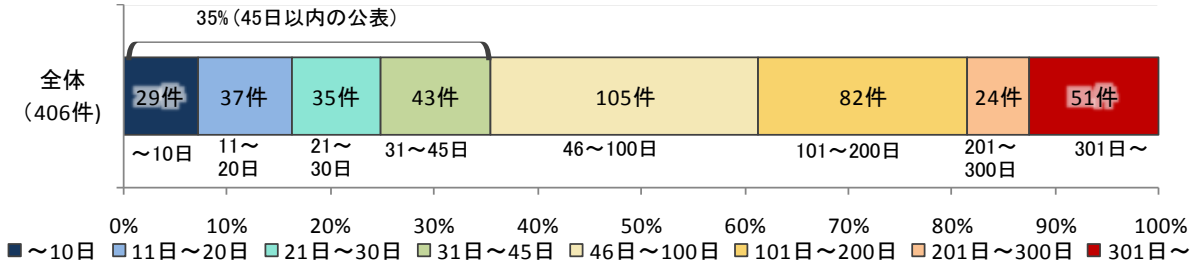


図1-7. ソフトウェア製品の脆弱性公表日数

表 1-2 に、国内の発見者、製品開発者から届出を受け、今四半期に公表した脆弱性を示します。オープンソースソフトウェアに関し公表したものが 3 件（表 1-2 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 1 件（表 1-2 の*2）ありました。

表 1-2.2010 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 II（警告）、CVSS 基本値=4.0～6.9				
1 (*1) (*2)	「Movable Type」におけるアクセス制限回避の脆弱性	ウェブログ作成管理システム「Movable Type」には、アクセス制限回避が可能な問題がありました。このため、第三者により、当該製品に保存されている情報を閲覧されたりする可能性がありました。	2010 年 1 月 6 日	5.5
2	「WebCalenderC3」におけるクロスサイト・スクリプティングの脆弱性	スケジューラ付カレンダーソフト「WebCalenderC3」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。	2010 年 1 月 12 日	4.3
3	「WebCalenderC3」におけるディレクトリ・トラバーサルの脆弱性	スケジューラ付カレンダーソフト「WebCalenderC3」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。	2010 年 1 月 12 日	5.0
4 (*1)	「OpenPNE」におけるアクセス制限回避の脆弱性	SNS 構築ソフト「OpenPNE」には、アクセス制限回避が可能な問題がありました。このため、遠隔の第三者により、当該製品で管理している情報を閲覧されたり、変更されたりする可能性がありました。	2010 年 3 月 5 日	5.8
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
5	「Oracle Application Server」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「Oracle Application Server」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2010 年 1 月 14 日	2.6
6 (*1)	tDiary 付属のプラグイン「tb-send.rb」におけるクロスサイト・スクリプティングの脆弱性	ウェブ日記支援ソフト tDiary 付属のプラグイン「tb-send.rb」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。	2010 年 2 月 25 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

（2）海外 CSIRT 等と連携して公表した脆弱性

JPCERT/CC が海外 CSIRT 等と連携して公表した脆弱性 20 件には、通常の脆弱性情報 13 件（表 1-3）と、対応に緊急を要する Technical Cyber Security Alert（表 1-4）の 7 件が含まれます。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 1-3.米国 CERT/CC[19]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	Linear eMerge のマネージメントコンポーネントにおけるサービス運用妨害 (DoS)	注意喚起として掲載
2	Microsoft Internet Explorer において任意のコードが実行される脆弱性	緊急案件として掲載
3	BIND 9 の DNSSEC 検証コードに脆弱性	複数製品開発者へ通知
4	Rockwell Automation Allen-Bradley MicroLogix PLC に複数の脆弱性	注意喚起として掲載
5	Linux カーネルの IPv6 jumbogram 処理に脆弱性	複数製品開発者へ通知
6	GNU gzip における複数の脆弱性	複数製品開発者へ通知
7	Panda Security ActiveScan におけるコンポーネントのデジタル署名を検証しない問題	注意喚起として掲載
8	APC Network Management Card 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
9	Internet Explorer において VBScript および Windows Help を使用する際に任意のコードが実行される脆弱性	緊急案件として掲載
10	libpng における圧縮された補助チャンクの処理に脆弱性	注意喚起として掲載
11	Microsoft Internet Explorer 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
12	IntelliCom NetBiter Config HICP 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
13	Broadcom NetXtreme 管理用ファームウェア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

表 1-4.米国 US-CERT[20]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	Oracle 製品における複数の脆弱性に対するアップデート
2	Microsoft Windows における EOT フォント エンジンおよび Adobe Flash Player 6 の脆弱性
3	Adobe Reader および Acrobat における複数の脆弱性に対するアップデート
4	Internet Explorer に複数の脆弱性
5	Microsoft 製品における複数の脆弱性に対するアップデート
6	Microsoft 製品における複数の脆弱性に対するアップデート
7	Internet Explorer に複数の脆弱性

[19] 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。
[20] United States Computer Emergency Readiness Team。米国の政府系 CSIRT。

2. ウェブサイトの脆弱性の処理状況の詳細

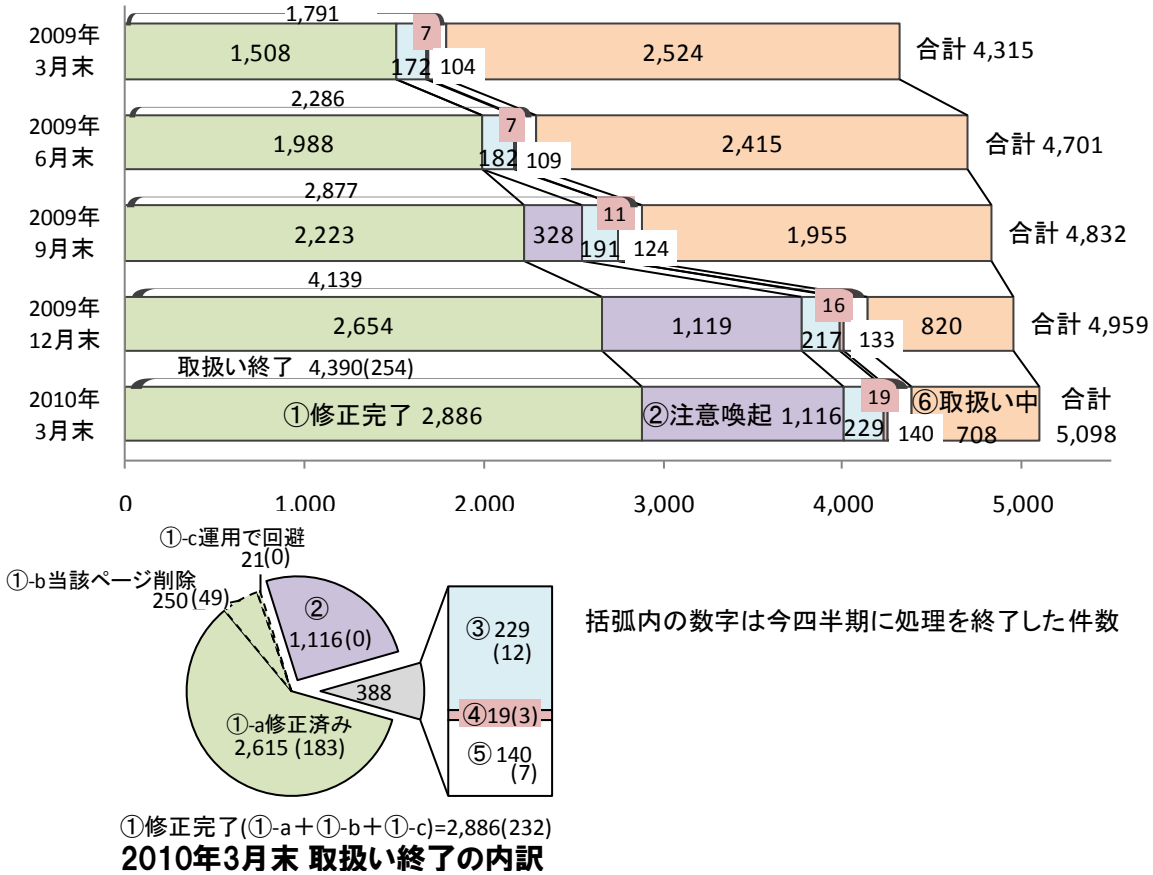
2.1 ウェブサイトの脆弱性の処理状況

ウェブサイトの脆弱性関連情報の届出について、処理状況を図 2-1 に示します。

図 2-1 に示すように、ウェブサイトの脆弱性について、今四半期中に処理を終了したものは 254 件[21]（累計 4,390 件）でした。このうち、「修正完了」したものは 232 件（累計 2,886 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 1,116 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 12 件（累計 229 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 3 件（累計 19 件）です。「不受理」としたものは 7 件（累計 140 件）でした。

取扱いを終了した累計 4,390 件のうち、「注意喚起」「連絡不可能」「不受理」を除く累計 3,115 件（71%）は、ウェブサイト運営者からの報告もしくは IPA の判断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 49 件（累計 250 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 21 件）でした。



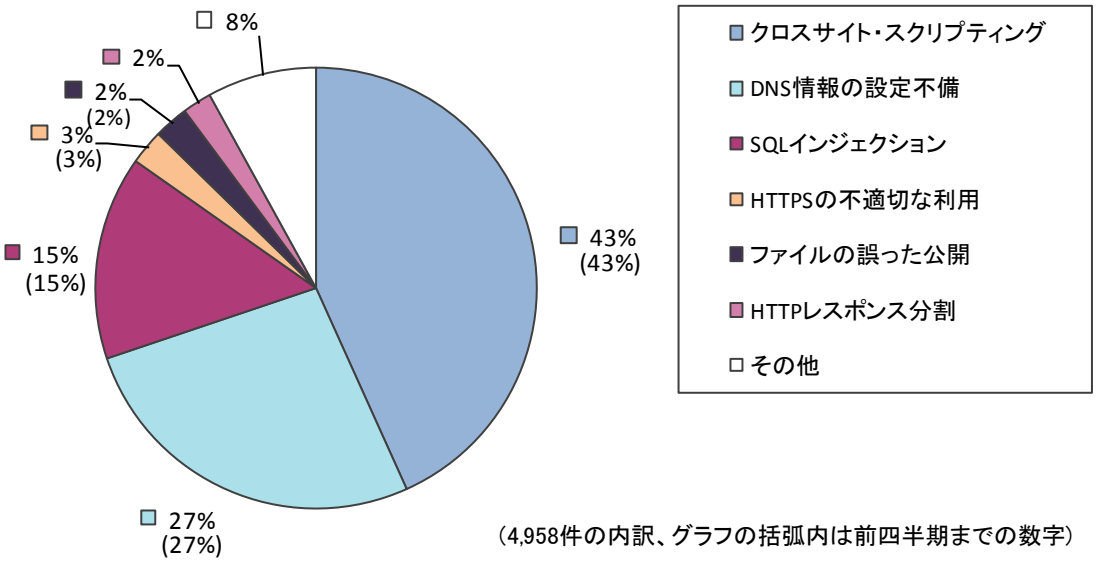
①修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
-a 修正済み	：	修正完了のうち、修正されたと判断したもの
-b 該当ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
-c 運用で回避	：	修正完了のうち、運用により被害を回避しているもの
②注意喚起	：	IPA による注意喚起で広く対策を促した後、処理を取りやめたもの
③脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
④連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
⑤不受理	：	告示で定める届出の対象に該当しないもの
⑥取扱い中	：	ウェブサイト運営者が調査、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

[21] 前四半期に注意喚起で終了したもの 3 件が今四半期に運営者からの報告を受け修正完了となりました。

2.2 ウェブサイトの脆弱性の種類と脅威

届出受付開始から今四半期までに IPA に届出のあったウェブサイトの脆弱性関連情報 5,098 件のうち、不受理のものを除いた 4,958 件について、種類別内訳を図 2-2 に、種類別の届出件数の推移を図 2-3 に、脅威別内訳を図 2-4 に示します[22]。



（4,958件の内訳、グラフの括弧内は前四半期までの数字）

図2-2.ウェブサイトの脆弱性 種類別内訳（届出受付開始から2010年3月末まで）

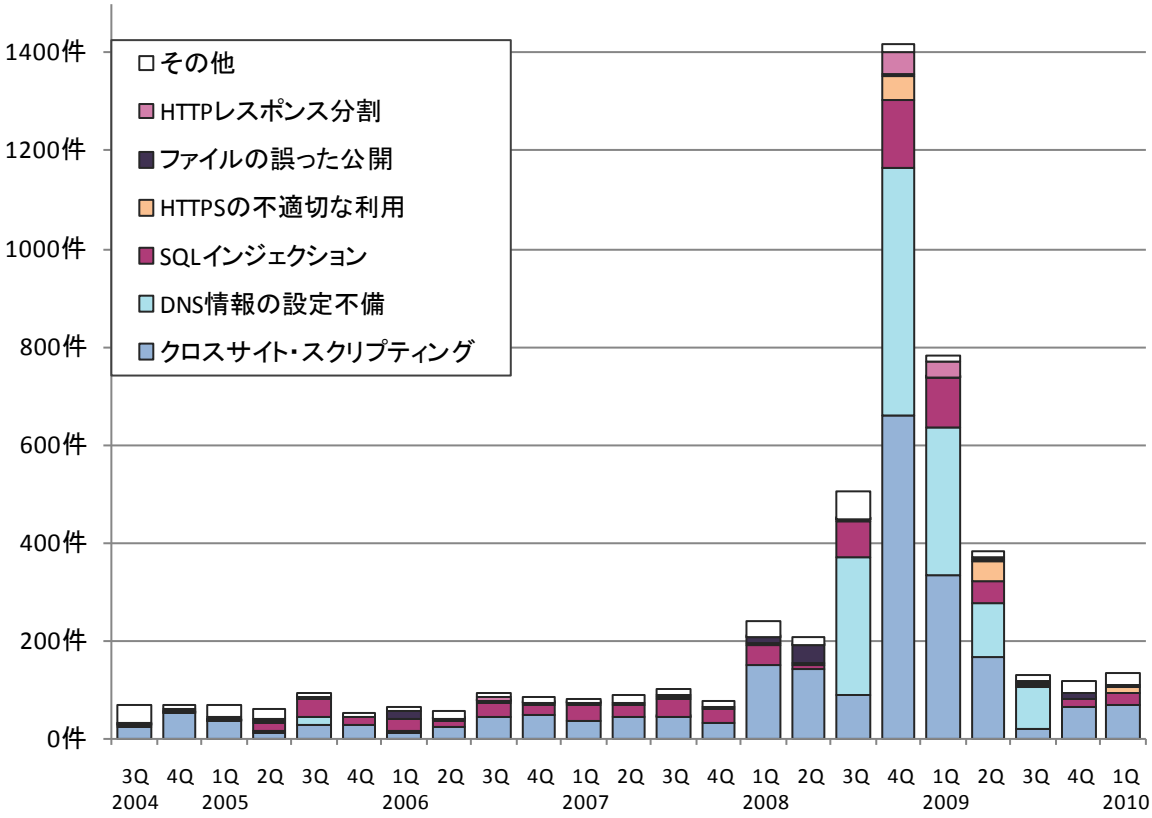
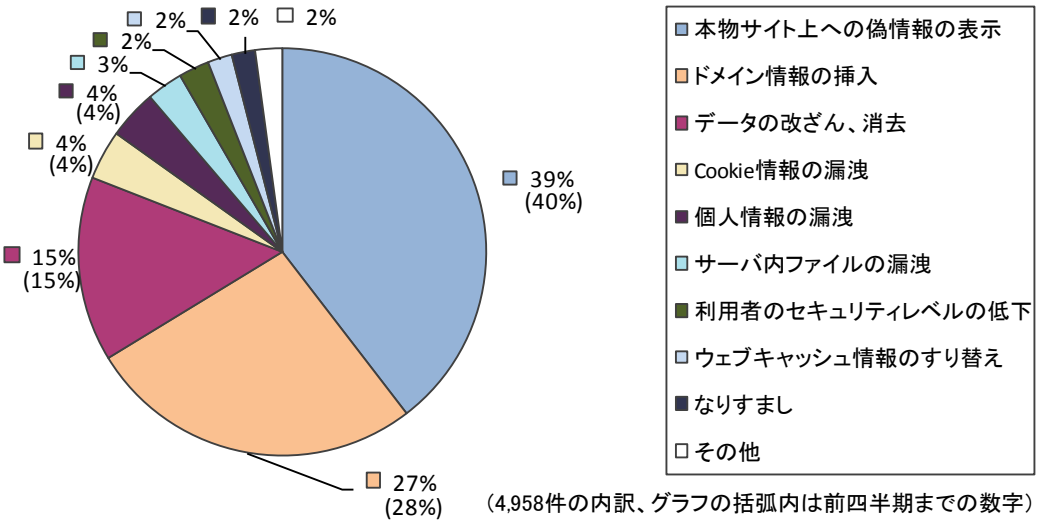


図2-3.ウェブサイトの脆弱性 種類別届出件数の推移（届出受付開始から2010年3月末まで）

[22] 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。



（4,958件の内訳、グラフの括弧内は前四半期までの数字）

図2-4.ウェブサイトの脆弱性 脅威別内訳（届出受付開始から2010年3月末まで）

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」だけで全体の 85%を占めています（図 2-2）。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、今四半期は届出がありませんでした（図 2-3）。

また「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」が脅威別内訳の 85%を占めています（図 2-4）。

2.3 ウェブサイトの脆弱性の修正状況

届出受付開始から今四半期までの届出の中で、修正完了したもの 2,886 件について、ウェブサイト運営者に脆弱性の詳細情報を通知してから修正されるまでに要した日数およびその傾向を、脆弱性の種類別に図 2-5 および図 2-6 に示します[23]。全体の 50%の届出が 30 日以内、全体の 70%の届出が 90 日以内に修正されています。

90 日以内の修正件数の割合

2008 1Q まで	2Q まで	3Q まで	4Q まで	2009 1Q まで	2Q まで	3Q まで	4Q まで	2010 1Q まで
77%	81%	80%	83%	80%	79%	79%	72%	70%

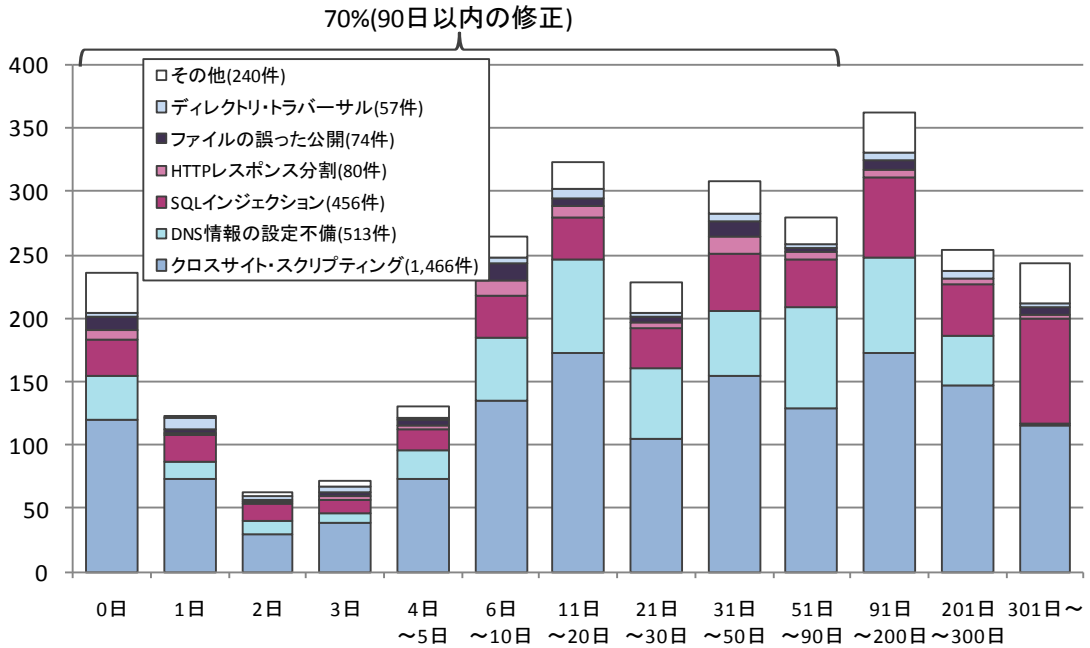


図2-5.ウェブサイトの修正に要した日数

[23] 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。

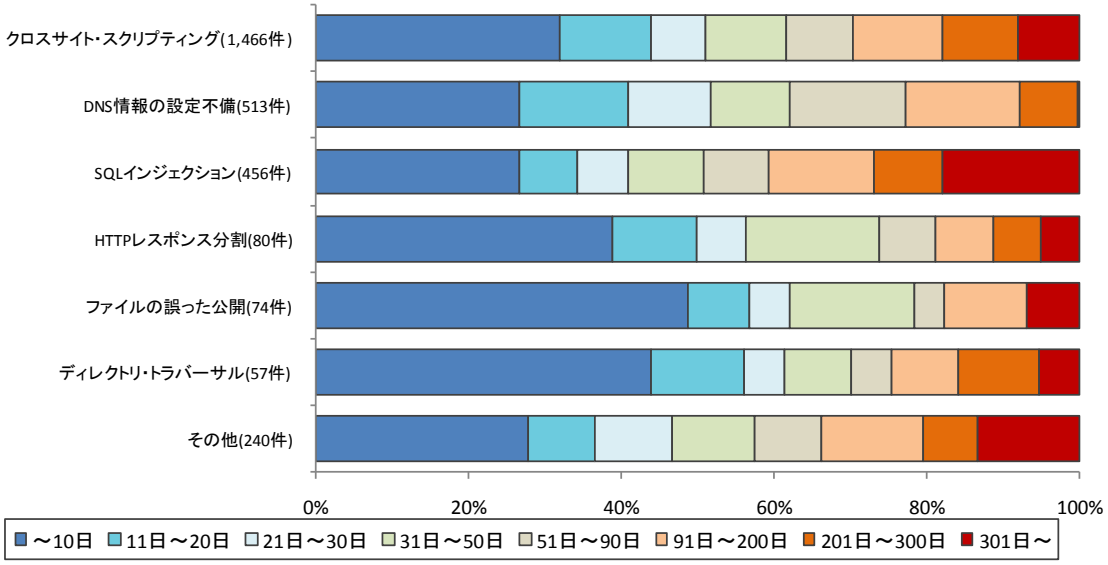


図2-6.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

3. 関係者への要望

脆弱性の修正を促進していくための、各関係者への要望は以下のとおりです。

（1）ウェブサイト運営者

多くのウェブサイト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：http://www.jpcert.or.jp/vh/ ）。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。

（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、My JVN（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

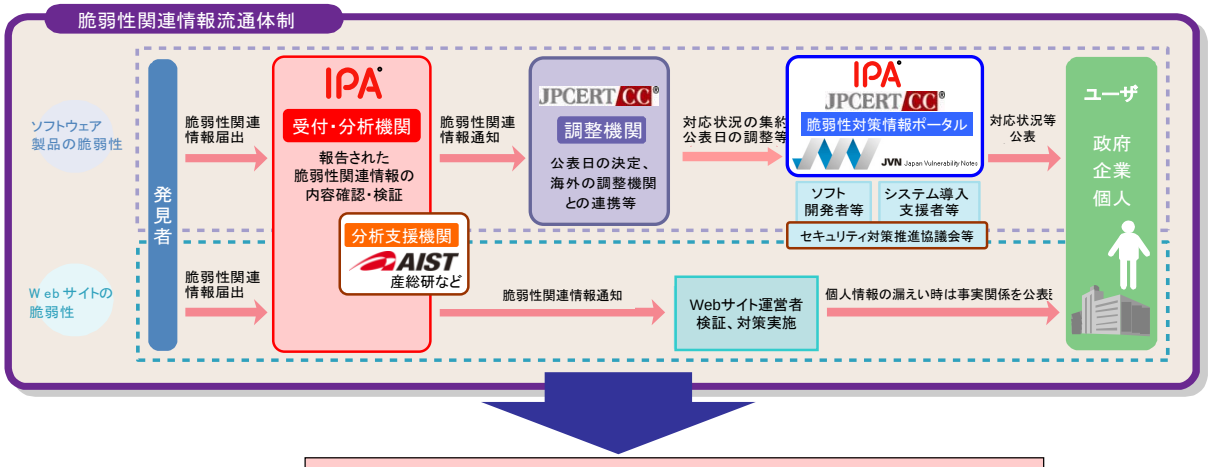
付表 2 ウェブサイト脆弱性の分類

	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個人情報等重要情報の流出や重要システムの停止を予防

※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：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