IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
JPCERT CC®

プレスリリース
2009 年 10 月 16 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 [2009 年第 3 四半期(7 月～9 月)]

～ウェブサイト運営者は脆弱性の修正に関して、十分な確認を！～

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、2009 年第 3 四半期（7 月～9 月）の脆弱性関連情報の届出状況[1]をまとめました。

(1)ウェブサイト運営者は脆弱性の修正に関して、十分な確認が必要です

IPA がウェブサイト運営者に脆弱性の存在を指摘し、運営者が脆弱性を修正後、脆弱性の発見者に修正完了の報告を行った際、2009 年 1 月から 9 月末までの修正完了 779 件のうち、発見者から 120 件（15%）の再指摘がありました（図 1）。その内訳は「修正不十分」が 69 件（9%）、「別の個所に脆弱性が存在」が 51 件（6%）でした。ウェブサイトの運営主体毎に算出した再指摘の割合をみると、個人（57%）、企業（23%）、団体（協会・社団法人、16%）などが高くなっています（図 2）。

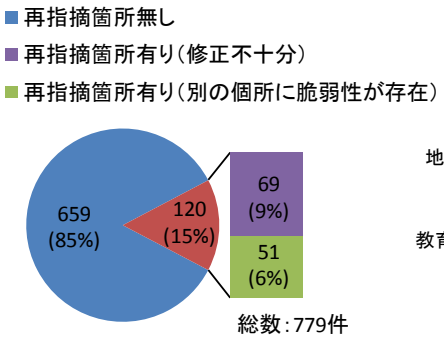


図1.発見者からの再指摘状況

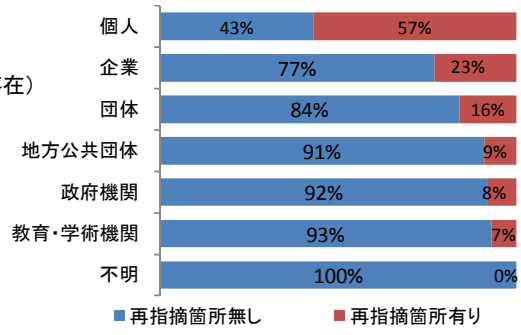


図2.運営者主体毎の発見者からの再指摘の割合

「修正不十分」の脆弱性の種類はクロスサイト・スクリプティングが 48 件（70%）、SQL インジェクションが 10 件（14%）、DNS 情報の設定不備が 8 件（12%）、HTTP レスポンス分割が 3 件（4%）となっています（図 3）。「別の個所に脆弱性が存在」は、それぞれ 45 件（88%）、4 件（8%）、1 件（2%）、1 件（2%）となっています（図 4）。

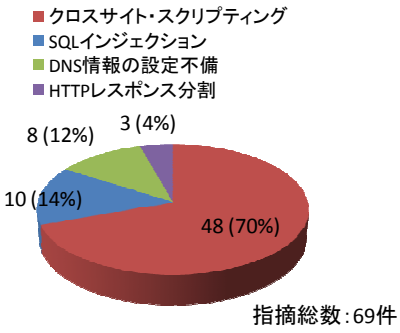


図3.修正不十分の脆弱性の種類

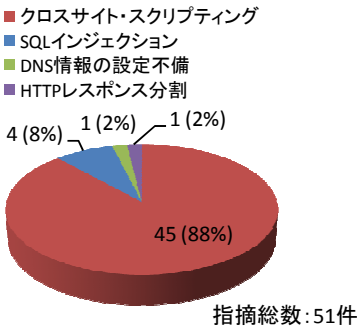


図4.別の個所に脆弱性が存在する脆弱性の種類

クロスサイト・スクリプティングの脆弱性は、情報を出力する処理に起因することが多く、一般的に、ウェブアプリケーションには出力処理が多数あることから、SQL インジェクションや DNS 情報の設定

[1] ソフトウェア等の脆弱性関連情報に関する届出制度：経済産業省告示に基づき、2004 年 7 月より開始しました。IPA は届出受付・分析、JPCERT/CC は国内の製品開発者などの関連組織との調整を行っています。

不備の脆弱性と比較して、修正した以外の箇所にも同様の脆弱性が存在する傾向があります。

脆弱性を修正する場合、脆弱性の修正の確認を十分にするとともに、別の箇所に、同様な脆弱性が存在していないかの確認も併せて実施してください。特にクロスサイト・スクリプティングのような、別の箇所に存在する可能性が高い脆弱性は、指摘された箇所を修正するだけでなく、ウェブサイト全体について確認する必要があります。場合によっては、設計に遡り見直すことも必要です。

(2)届出件数の累計が 5,826 件となりました

2009 年第 3 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 39 件、ウェブアプリケーション（ウェブサイト）に関するもの 131 件、合計 170 件でした（表 1）。

表 1. 2009 年第 3 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	**39** 件	**994** 件
ウェブサイト	**131** 件	**4,832** 件
合計	**170** 件	**5,826** 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 994 件、ウェブサイトに関するもの 4,832 件[2]、合計 5,826 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（図 5）。2008 年第 3 四半期ごろから DNS の設定不備、SQL インジェクションの脆弱性の届出が増加し、2008 年第 4 四半期に一時的にクロスサイト・スクリプティングの届出が激増しましたが、近年はウェブサイトに関する届出が減少傾向です。

1 就業日あたりの届出件数は 2009 年第 3 四半期末で 4.56 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
累計届出件数[件]	1,310	2,045	2,322	2,885	4,375	5,227	5,656	5,826
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

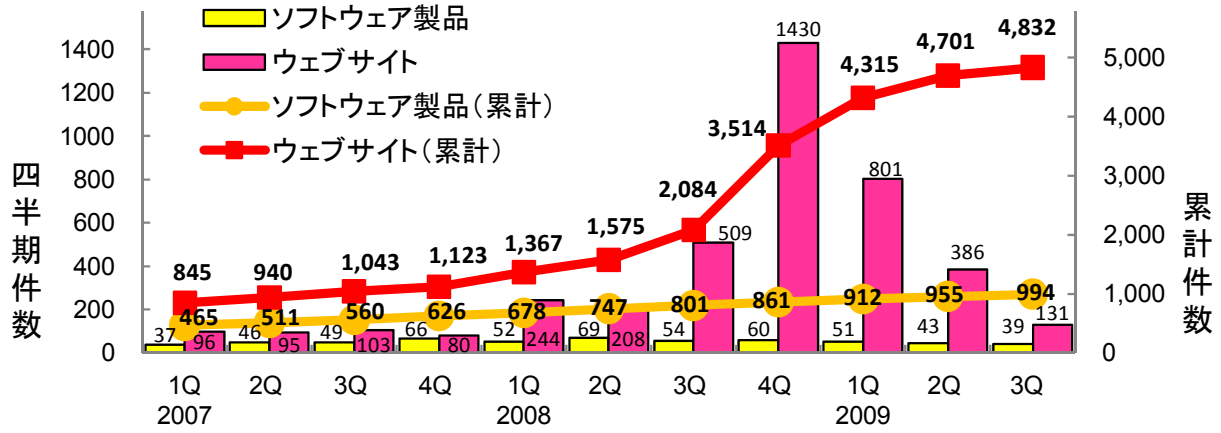


図5.脆弱性関連情報の届出件数の四半期別推移

■ 本件に関するお問い合わせ先
IPA セキュリティセンター 山岸／渡辺
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

[2] 2009/1Qに届けられた4件が他の届出と同一の脆弱性と今四半期に判断したため、2009/1Qの届出件数を4件減らしました。

別紙 1

1.ソフトウェア製品の脆弱性の処理状況

2009 年第 3 四半期のソフトウェア製品の脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものが 17 件（累計 384 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 0 件（累計 35 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 5 件[3]（累計 148 件）でした。これらの取扱いを終了したものの合計は 22 件（累計 584 件）です（表 3）。

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	17 件	384 件
	個別対応	0 件	17 件
脆弱性ではない		0 件	35 件
不受理		5 件	148 件
合計		22 件	584 件

この他、海外の CSIRT[4]から JPCERT/CC が連絡を受けた 19 件（累計 441 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 6 に示します。

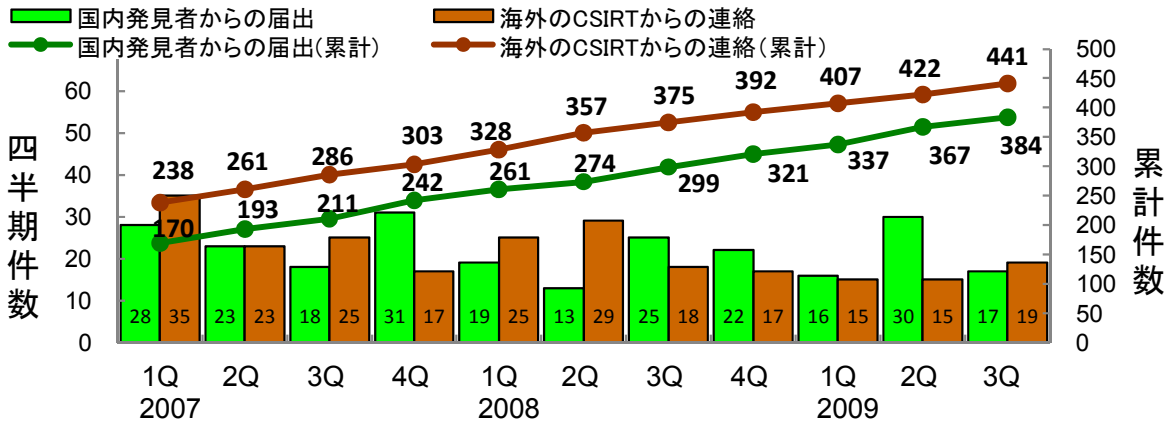


図6.ソフトウェア製品の脆弱性対策情報の公表件数

1.1 JVN で公表した主な脆弱性対策情報

今四半期は、「FreeNAS」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[5]、「ATOK」におけるスクリーンロックの制限回避が可能な脆弱性[6]、「SugarCRM」における SQL インジェクションの脆弱性[7]、「Microsoft Windows」におけるバッファオーバーフローの脆弱性[8]などの脆弱性対策情報を JVN で公表しました。

1.2 JVN が CVE 互換の認定プロセスに入りました

共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）[9]は、個別製品の脆弱性を対象とした識別子です。MITRE 社では、CERT/CC や HP、IBM、OSVDB、Red Hat、Symantec など 80 を超える組織と連携し、脆弱性情報の収集と重複のない採番を行っています。1999 年の運用開始以来、2009 年 9 月 29 日に 10 周年を迎えました。

---

[3] 今四半期の届出の中で不受理とした 2 件、前期までの届出の中で今期に不受理とした 3 件の合計です。
[4] 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。
[5] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.1、別紙 P.8 表 1-2 項番 2 を参照下さい。
[6] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.2、別紙 P.8 表 1-2 項番 3 を参照下さい。
[7] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=6.5、別紙 P.9 表 1-2 項番 10 を参照下さい。
[8] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=6.8、別紙 P.9 表 1-2 項番 11 を参照下さい。
[9] 脆弱性情報を一意に特定するための標準仕様で、脆弱性に対して共通の識別子（CVE-ID）を付与したリストです。米国の非営利団体の MITRE 社が管理・運用しています。概要は「共通脆弱性識別子 CVE の概説」を参照下さい。http://www.ipa.go.jp/security/vuln/CVE.html

IPA と JPCERT/CC が共同で運営している JVN（Japan Vulnerability Notes）[10]も連携に参画しており「CVE 情報源サイト」の一つとして掲載されています[11]。CVE との連携の意思を明確に示すため、2008 年 12 月に JVN の「CVE 互換宣言」を行いました。**さらに、2009 年 9 月に、「CVE 互換」の認定を受けるため「CVE 互換要件評価フォーム」を MITRE 社へ提出しました[12]。**審査終了後、「CVE 互換」が認定される予定です。

http://cve.mitre.org/compatible/questionnaires/104.html

今後も共通基準の導入を進めることにより、国内外の脆弱性対策情報流通の促進を図ると共に、利用者側の客観的・効率的な脆弱性対策を目指した利活用基盤を整備していきます。

2.ウェブサイトの脆弱性の処理状況

2009 年第 3 四半期のウェブサイトの脆弱性の処理状況は、IPA が通知を行い、ウェブサイト運営者が修正を完了したものは 235 件（累計 2,223 件）、IPA が注意喚起等を行い処理を終了したものは 328 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が 9 件、ウェブサイト運営者と連絡が不可能なものが 4 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 15 件[13]でした。

これらの取扱いを終了したものの合計は 591 件（累計 2,877 件）です（表 4）。これらのうち、修正完了件数の期別推移を図 7 に示します。

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	**235** 件	**2,223** 件
注意喚起	**328** 件	**328** 件
脆弱性ではない	**9** 件	**191** 件
連絡不可能	**4** 件	**11** 件
不受理	**15** 件	**124** 件
合計	**591** 件	**2,877** 件

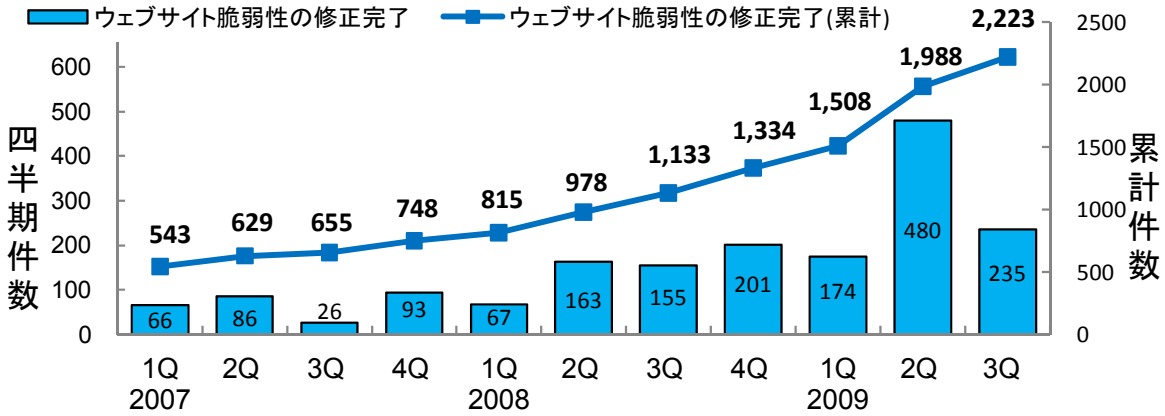


図7.ウェブサイトの脆弱性の修正完了件数

2.1 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

今四半期に脆弱性の届出を受理した 131 件の対象ウェブサイトの運営主体別内訳は、企業合計が 99 件（76%）、団体（協会・社団法人）が 13 件（10%）、地方公共団体が 8 件（6%）、個人が 3 件（2%）、その他、不明が 8 件（6%）（図 8）となっています。

また、これらの脆弱性の種類は、DNS の設定不備（DNS キャッシュポイズニングの脆弱性）が 88

[10] 脆弱性対策情報ポータルサイト。国内で利用されている製品の脆弱性対策情報を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。http://jvn.jp/
[11] http://cve.mitre.org/data/refs/index.html#sources
[12] http://cve.mitre.org/compatible/organizations.html#j
[13] 今期の届出の中で不受理としたものは 0 件、前期までの届出の中で今期に不受理としたものは 15 件です。

件（67%）、クロスサイト・スクリプティングが 19 件（15%）、HTTPS の不適切な利用が 6 件（5%）などとなっています（図 9）。

ウェブサイト開発者は脆弱性を作りこ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。届出件数の多い、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いです。

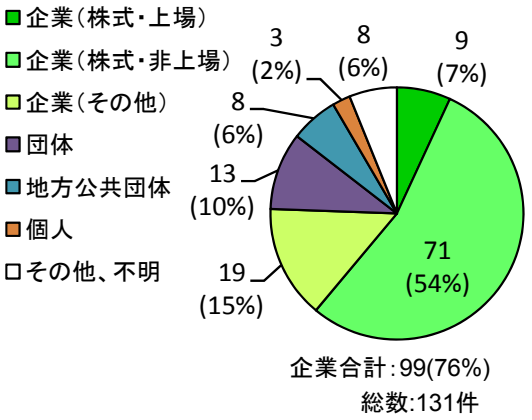


図8.ウェブサイトの運営主体（2009年3Q）

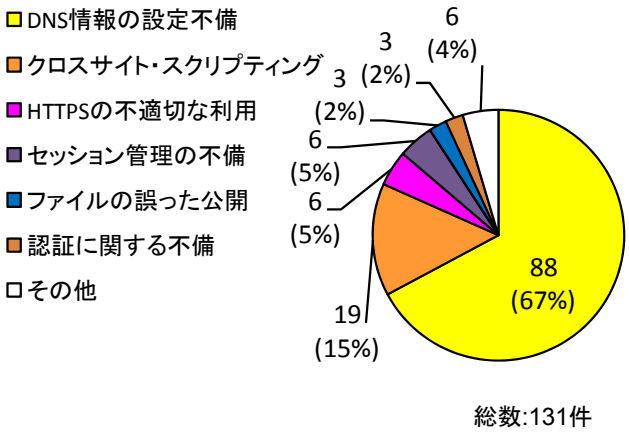
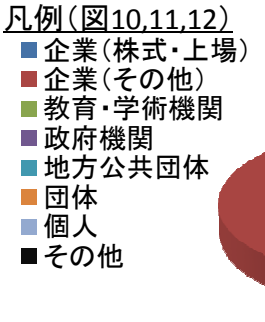


図9.ウェブサイトの脆弱性の種類（2009年3Q）

2.2 古いバージョンのソフトウェアを使い続けているウェブサイトへの注意喚起を実施

2008 年頃より、ソフトウェア製品を利用しているウェブサイトに対して「製品開発者から既に脆弱性対策を施したバージョンが公表されているにも関わらず、古いバージョンを使い続けている」という旨の届出が増加しています。今四半期には、「EC-CUBE の古いバージョンを利用しているウェブサイトへの注意喚起[14]」及び「Namazu の古いバージョンを利用しているウェブサイトへの注意喚起[15]」を実施しました。

クロスサイト・スクリプティングの脆弱性が指摘された古い「EC-CUBE」を利用しているウェブサイトに対する届出では、中小規模の企業（株式・上場以外のその他）の占める割合が 92%（図 10）、古い「Namazu」を利用しているウェブサイトに対する届出では、教育・学術機関の占める割合が 16%、地方公共団体が 27%となっています（図 11）。クロスサイト・スクリプティング全体では、それぞれの占める割合が 45%、5%、17%となっていますので、中小規模の企業、教育・学術機関、地方公共団体で当該製品を使い続けている割合が高いようです（図 12）。



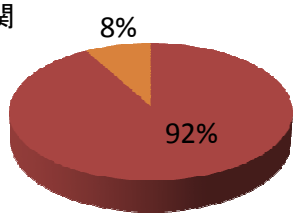


図10.古い「EC-CUBE」を使用

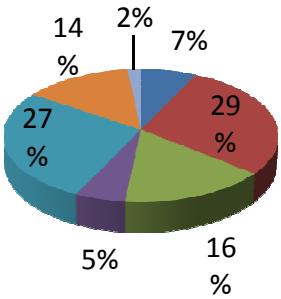


図11.古い「Namazu」を使用

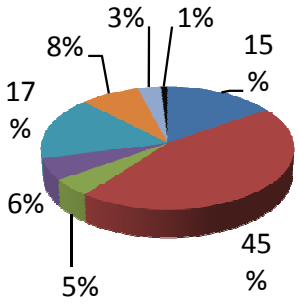


図12.クロスサイト・スクリプティング全体の届出

[14] http://www.ipa.go.jp/security/vuln/documents/2009/200907_ec-cube.html
[15] http://www.ipa.go.jp/security/vuln/documents/2009/200908_namazu.html

この他、今四半期には「OpenSSL の古いバージョンを利用しているウェブサイトへの注意喚起[16]」も行いました。近年、脆弱性の公表から、その脆弱性を狙った攻撃が発生するまでの間隔が短くなっています。ソフトウェア製品を運用するウェブサイトの運営者も、そのソフトウェア製品を狙った攻撃を受ける可能性や、攻撃が実際の被害に結び付く可能性が高まっています。

ウェブサイト運営者は、自組織のウェブサイトが使用しているソフトウェア製品を把握し、その脆弱性対策情報を収集してください。未対策の脆弱性があった場合、パッチの適用やバージョンアップなどの対策を施して下さい。また、ソフトウェア製品の更新手順をドキュメント化することや、更新確認用のシステムの整備、対策を外部に委託する際の調整など、継続的な対策のための環境を整備することも重要です。

2.3 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、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およびウェブサイトの脆弱性検査、脆弱性対策の早急な実施を改めて推奨する注意喚起を行いました。

攻撃の現状を把握する実例として、IPA が公開している「脆弱性対策情報データベース JVN iPedia[17]」について、2009 年 4 月から 7 月までのアクセスログを、IPA が無償で公開している「ウェブサイトの脆弱性検出ツール iLogScanner[18]」で解析した事例を公開しましたが、図 13 に示すように 8 月以降も攻撃が継続しています。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。

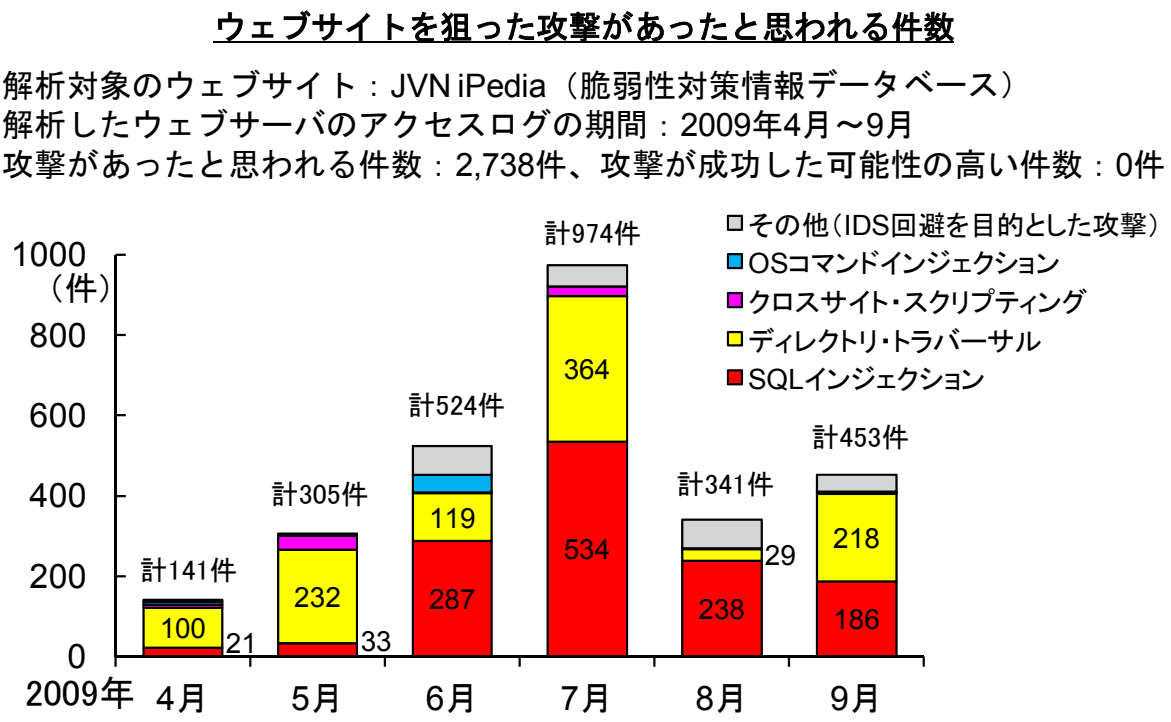


図13. SQLインジェクション検出ツール「iLogScanner」での解析事例

[16] http://www.ipa.go.jp/security/vuln/documents/2009/200909_openssl.html
[17] 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/
[18] 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

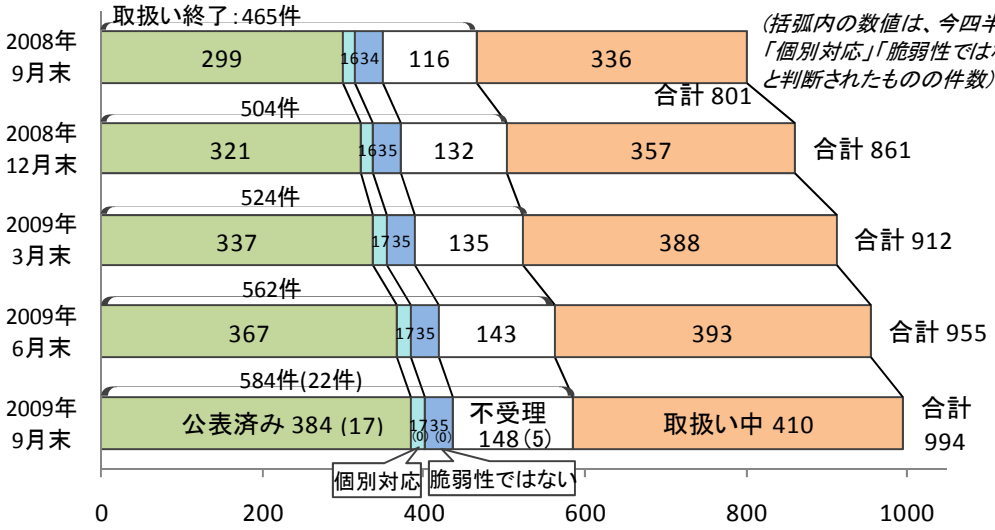
別紙 2

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 17 件（累計 384 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 0 件（累計 35 件）、「不受理」としたものは 5 件（累計 148 件）、取扱中は 410 件です。



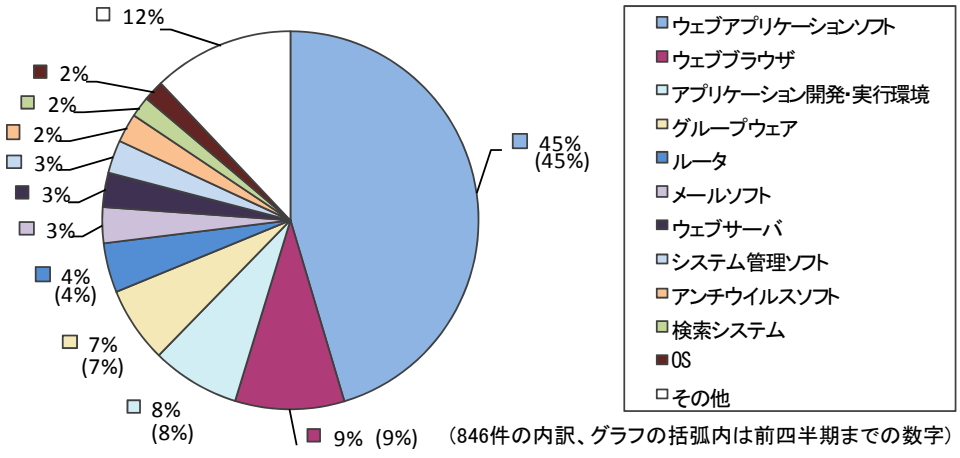
公表済み	：JVN で脆弱性への対応状況を公表したもの
個別対応	：製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない	：製品開発者により脆弱性ではないと判断されたもの
不受理	：告示で定める届出の対象に該当しないもの
取扱い中	：製品開発者が調査、対応中のもの

図 1-1.ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

1.2 届出られた製品の種類

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 994 件のうち、不受理のものを除いた 846 件の製品種類別の内訳を図 1-2 に示します。

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



（846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2009年9月末まで）

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 994 件のうち、不受理のものを除いた 846 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 9 件ありました。2006 年頃までは上昇傾向でしたが、2008 年以降は徐々に下降して推移しています。

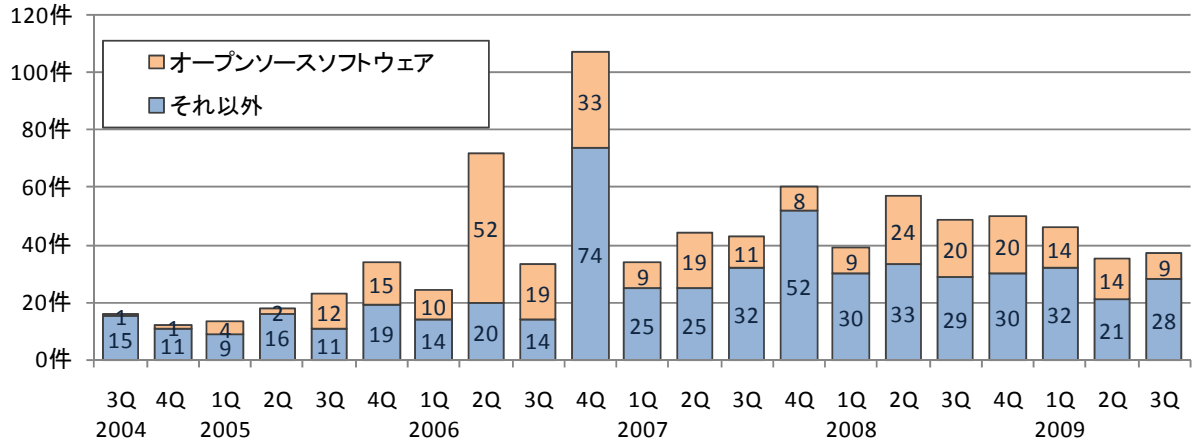
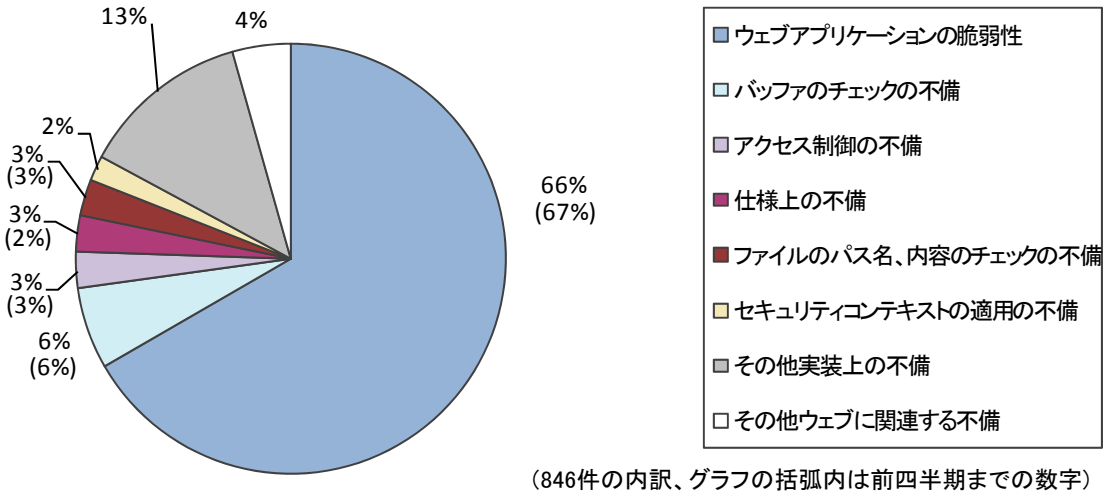


図1-3.オープンソースソフトウェアの脆弱性の届出件数 （846件の内訳）

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 に届出られたソフトウェア製品に関する脆弱性関連情報 994 件のうち、不受理のものを除いた 846 件の原因別[19]の内訳を図 1-4 に、原因別の届出件数の推移を図 1-5 に、脅威別の内訳を図 1-6 に示します。

図 1-4 に示すように、脆弱性の原因は「ウェブアプリケーションの脆弱性」が最多であり、図 1-6 に示すように、脅威についても「任意のスクリプト実行」が最多となっています。この傾向は図 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あっても、ウェブブラウザから管理、使用するものが多くあり、そこに脆弱性が存在するため、比較的見つけやすい事が理由と考えられます。



（846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2009年9月末まで）

[19] それぞれの脆弱性の詳しい説明については付表 1 を参照してください。

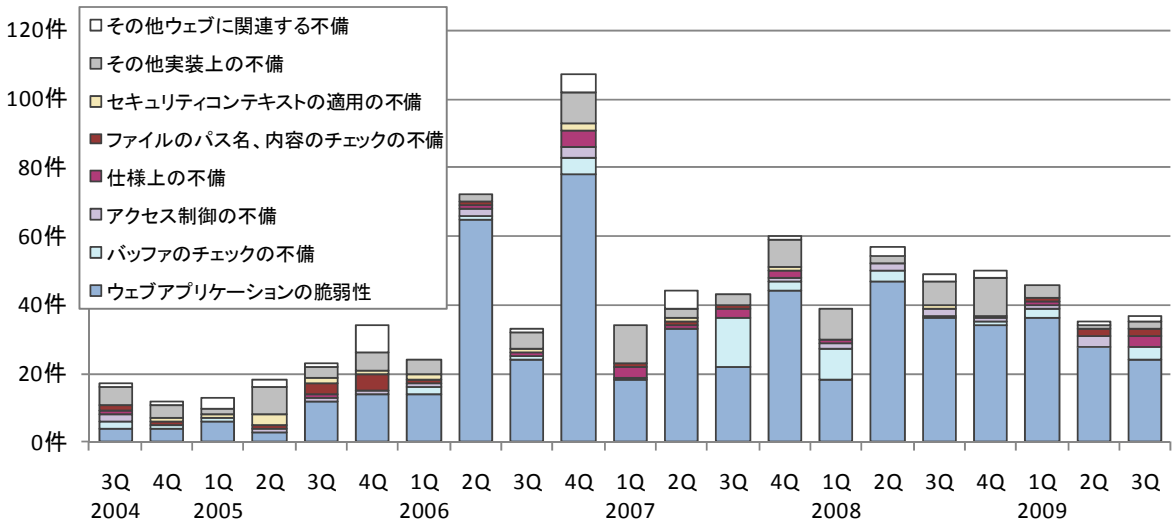
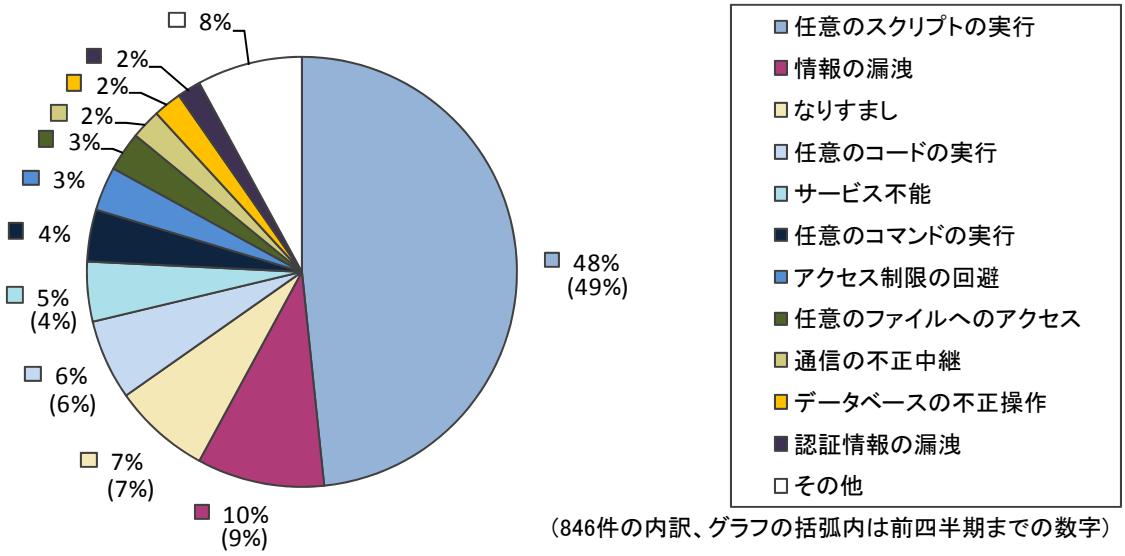


図1-5. ソフトウェア製品の脆弱性 原因別届出件数の推移（届出受付開始から2009年9月末まで）



（846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2009年9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[20]の協力のもと、海外の製品開発者との調整を行っています。これらの脆弱性関連情報に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）において公表しています。（URL： http://jvn.jp/ ）

表 1-1. 脆弱性関連情報の提供元別 脆弱性公表件数

	情報提供元	今期	累計
①	国内の発見者から IPA に届出があったもの、および、製品開発者自身から自社製品の脆弱性、対策方法について連絡を受けたもの	17 件	384 件
②	海外 CSIRT 等と連携して公表したもの	19 件	441 件
	合計	36 件	825 件

[20] CSIRT（Computer Security Incident Response Team）は、コンピュータセキュリティに関するインシデント（事故）への対応や調整、サポートをするチームのことです。

（1）国内の発見者および製品開発者から届出があり公表した脆弱性

届出受付開始から 2009 年 9 月末までの届出について、脆弱性関連情報の届出（表 1-1 の①）を受理してから製品開発者が対応状況を公表するまでに要した日数を図 1-7 に示します。届出受付開始から各四半期末までの 45 日以内に公表される件数が 35%であり、公表するまでに要した日数は 2008 年第 3 四半期からほぼ変わらずに推移しています。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
32%	32%	33%	34%	35%

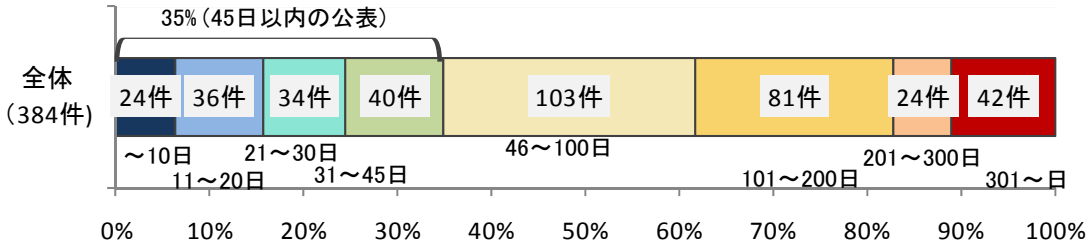


図1-7. ソフトウェア製品の脆弱性公表日数

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 7 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 1-2.2009 年第 3 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.				
1	株式会社ディーアイシー製「yoyaku_v41」における OS コマンド・インジェクションの脆弱性	施設予約管理ソフト「yoyaku_v41」には、リクエスト処理に問題がありました。このため、yoyaku_v41 を設置しているサーバ上で、サーバの権限で任意の OS コマンドを実行される可能性がありました。項番 4 で修正された問題とは異なります。	2009 年 7 月 31 日	7.5
2 (*1)	「FreeNAS」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	ファイルサーバ OS「FreeNAS」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 FreeNAS の設定を変更されたりデータを削除される可能性がありました。	2009 年 8 月 5 日	7.1
3	「ATOK」におけるスクリーンロックの制限回避が可能な脆弱性	日本語入力システム「ATOK」には、スクリーンロックの制限を回避可能な脆弱性がありました。このため、ローカルシステムアカウントの権限で、任意のコマンドやプログラムを実行される可能性がありました。	2009 年 9 月 2 日	7.2

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
4	株式会社ディーアイシー製「yoyaku_v41」における OS コマンド・インジェクションの脆弱性	施設予約管理ソフト「yoyaku_v41」には、リクエスト処理に問題がありました。このため、yoyaku_v41 を設置しているサーバ上で、サーバの権限で任意の OS コマンドを実行される可能性がありました。項番 1 で修正された問題とは異なります。	2009 年 9 月 11 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
5	「shiromuku(fs6)DIARY」におけるクロスサイト・スクリプティングの脆弱性	ウェブ日記作成支援ソフト「shiromuku(fs6)DIARY」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。	2009 年 7 月 14 日	4.3
6 (*2)	futomi's CGI Cafe 製「RevoCounter CGI (アニメーションカウンター)」におけるクロスサイト・スクリプティングの脆弱性	アニメーションカウンターソフト「RevoCounter CGI」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。	2009 年 7 月 24 日	4.3
7 (*1)	「MySQL Connector/J」における SQL インジェクションの脆弱性	MySQL データベース用ドライバソフト「MySQL Connector/J」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。	2009 年 7 月 29 日	6.8
8	「ColdFusion」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ソフト「ColdFusion」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。	2009 年 8 月 19 日	4.3
9 (*1)	「サイトカレンダ mycaljp」におけるクロスサイト・スクリプティングの脆弱性	Geeklog 用カレンダープラグイン「サイトカレンダ mycaljp」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。	2009 年 8 月 21 日	4.3
10 (*1)	「SugarCRM」における SQL インジェクションの脆弱性	顧客管理システム「SugarCRM」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。	2009 年 8 月 24 日	6.5
11	「Microsoft Windows」におけるバッファオーバーフローの脆弱性	Microsoft Windows の「Windows Media Format Runtime」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、利用者のコンピュータ上で任意のコードを実行される可能性がありました。	2009 年 9 月 9 日	6.8
12 (*1)	「XF-Section」におけるクロスサイト・スクリプティングの脆弱性	XOOPS 用コンテンツカテゴリ分け機能などのモジュール「XF-Section」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す。	2009 年 9 月 17 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
13	複数の phpspot 製品におけるクロスサイト・スクリプティングの脆弱性	phpspot が提供する掲示板ソフトウェア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。	2009 年 9 月 18 日	4.3
14	複数の phpspot 製品におけるディレクトリ・トラバーサルの脆弱性	phpspot が提供する掲示板ソフトウェアなどの複数の製品には、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、本ソフトが設置されているサーバ内のファイルを閲覧される可能性がありました。	2009 年 9 月 18 日	5.0
脆弱性の深刻度=レベルⅠ（注意）、CVSS 基本値=0.0～3.9				
15 (*1)	「FreeNAS」におけるクロスサイト・スクリプティングの脆弱性	ファイルサーバ OS「FreeNAS」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。	2009 年 8 月 5 日	2.6
16 (*1)	「bingo!CMS core」および「bingo!CMS」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	コンテンツ管理システム「bingo!CMS core」および「bingo!CMS」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 bingo!CMS core および bingo!CMS の設定を変更されたり、当該製品で作成したコンテンツを改ざんされる可能性がありました。	2009 年 8 月 27 日	2.6
17	「Opera」におけるサードパーティ Cookie の取り扱いに関する問題	ウェブブラウザ「Opera」には、サードパーティ Cookie の取り扱いに問題がありました。このため、第三者によりアクセス履歴を追跡される可能性がありました。	2009 年 9 月 17 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 19 件には、通常の脆弱性情報 12 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[21]等と連携した脆弱性関連情報および対応状況

項番	脆弱性	対応状況
1	ISC DHCP dhclient における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
2	XML 署名の検証において認証回避が可能な問題	複数製品開発者へ通知
3	Mozilla Firefox 3.5 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
4	Microsoft Office Web コンポーネントのスプレッドシート ActiveX コントロールに脆弱性	緊急案件として掲載
5	Adobe Flash に脆弱性	注意喚起として掲載
6	ISC BIND 9 におけるサービス運用妨害 (DoS) の脆弱性	緊急案件として掲載
7	複数の XML ライブラリの実装に脆弱性	複数製品開発者へ通知
8	Microsoft Internet Information Services FTP サーバ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
9	複数の TCP の実装におけるサービス運用妨害 (DoS) の脆弱性	複数製品開発者へ通知
10	Cyrus IMAPd 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
11	Windows SMB version 2 に脆弱性	緊急案件として掲載
12	Nginx ngx_http_parse_complex_uri() にバッファアンダーランの脆弱性	複数製品開発者へ通知

表 1-4.米国 US-CERT[22]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 Video ActiveX コントロールにおけるバッファオーバーフローの脆弱性
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	Adobe Flash Player および他の Adobe 製品に影響を及ぼす Adobe Flash の脆弱性
4	Microsoft Windows、Internet Explorer および Active Template Library (ATL) における脆弱性
5	Apple 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	Microsoft 製品における複数の脆弱性に対するアップデート

[21] 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。

[22] 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

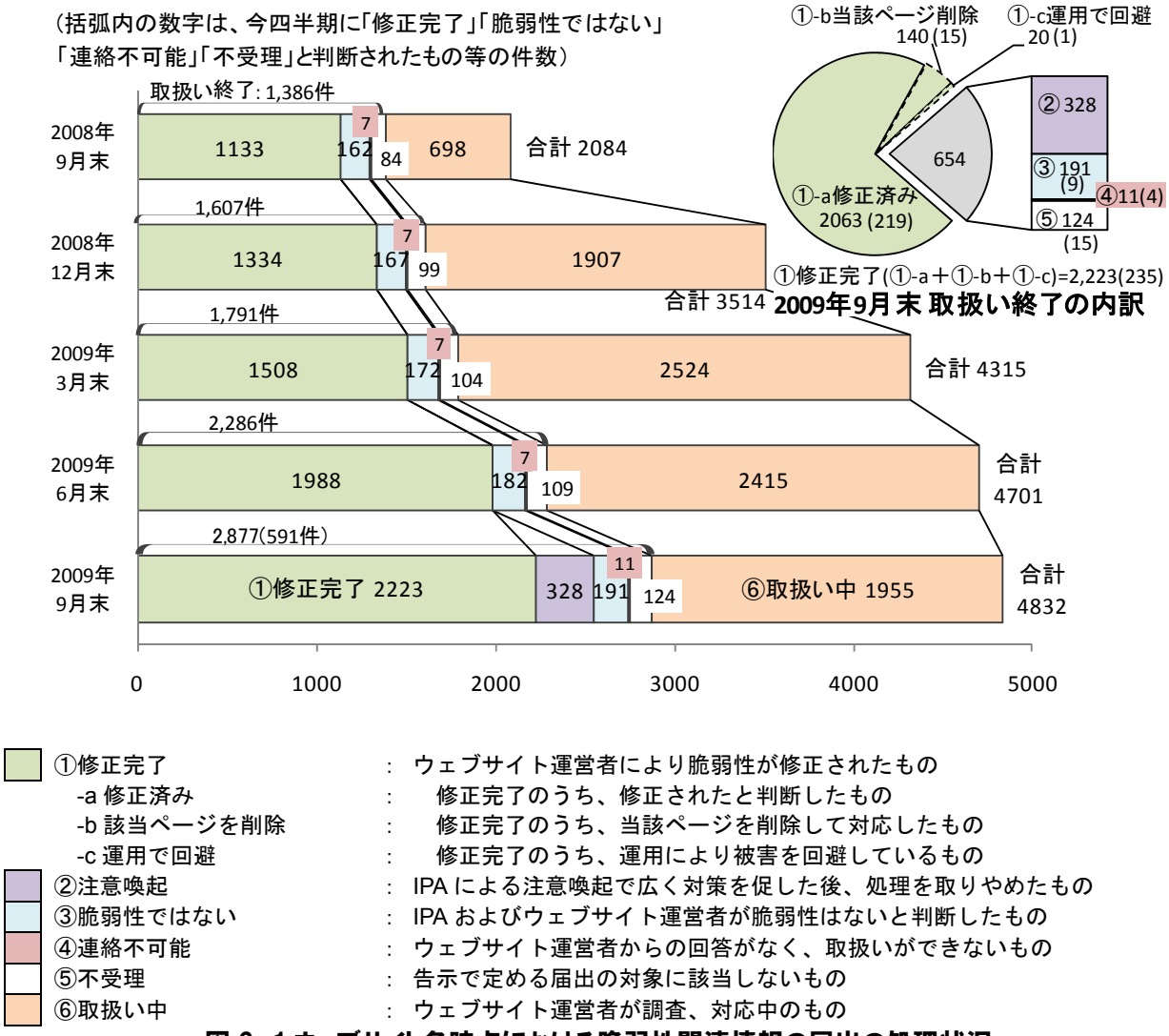
2.1 ウェブサイトの脆弱性の処理状況

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 591 件（累計 2,877 件）でした。このうち、「修正完了」したものは 235 件（累計 2,223 件）、ガイドライン改訂により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 328 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 9 件（累計 191 件）でした。なお、メールでウェブサイト運営者と連絡が取れない場合は、電話や郵送手段で連絡を試みたり、レンタルサーバ会社と連絡を試みたりしていますが、それでも、ウェブサイト運営者から回答がなく「連絡不可能」なものは 4 件(累計 11 件)です。「不受理」としたものは 15 件（累計 124 件）でした。

取扱いを終了した累計 2,877 件のうち、「注意喚起」「連絡不可能」「不受理」を除く累計 2,414 件（84%）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事を確認しました。

「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 140 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 20 件）でした。

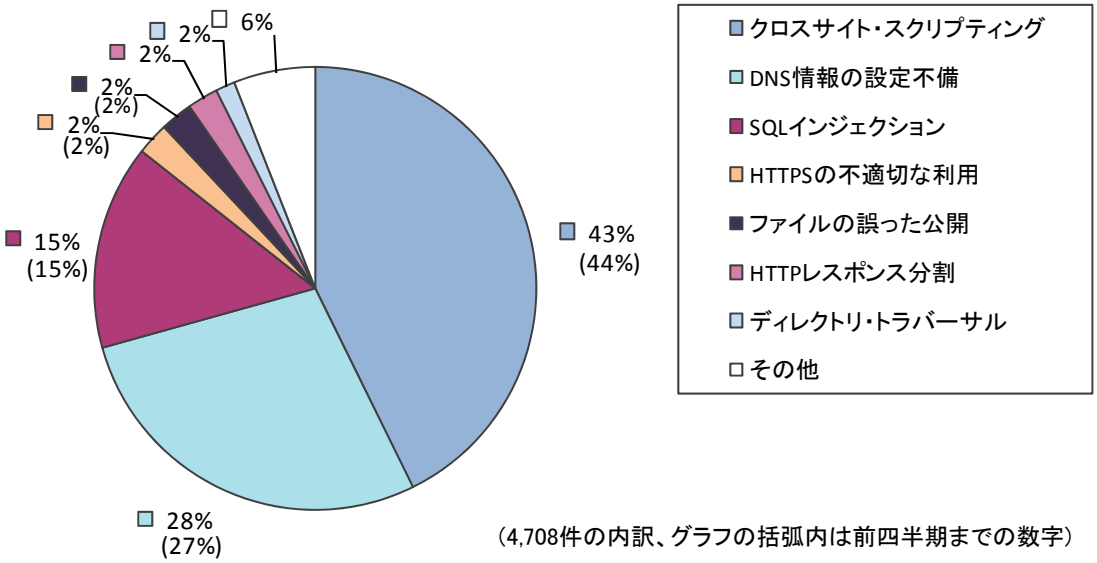


①修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
-a 修正済み	：	修正完了のうち、修正されたと判断したもの
-b 該当ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
-c 運用で回避	：	修正完了のうち、運用により被害を回避しているもの
②注意喚起	：	IPA による注意喚起で広く対策を促した後、処理を取りやめたもの
③脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
④連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
⑤不受理	：	告示で定める届出の対象に該当しないもの
⑥取扱い中	：	ウェブサイト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

2.2 ウェブサイトの脆弱性の種類と脅威

届出受付開始から今四半期末までに IPA に届出られたウェブサイトの脆弱性関連情報 4,832 件のうち、不受理のものを除いた 4,708 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[23]。



（4,708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2009年9月末まで）

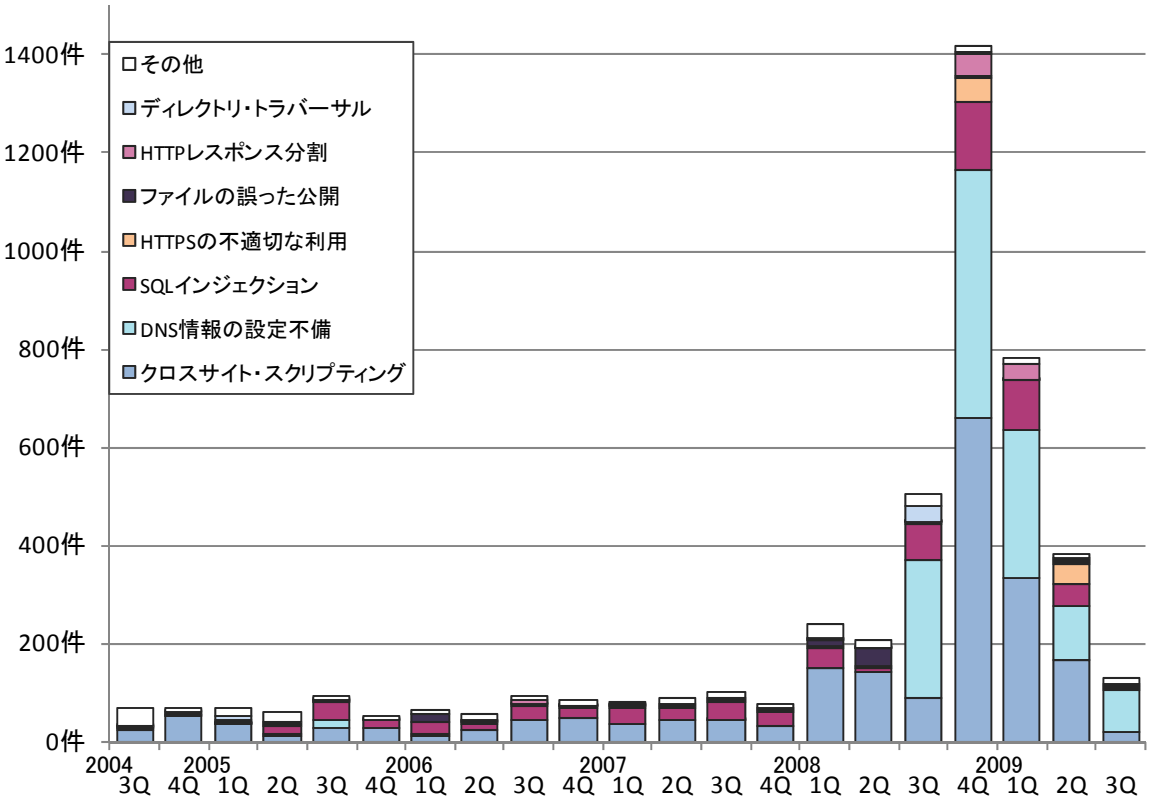
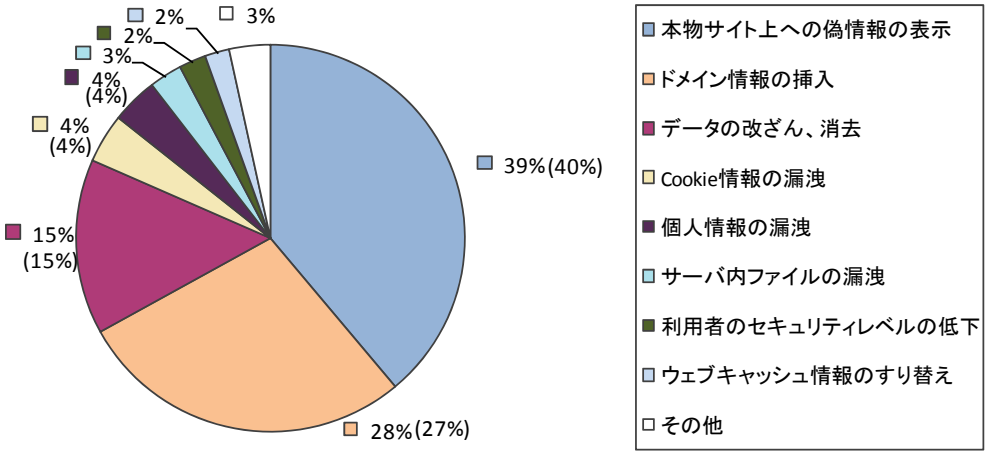


図2-3.ウェブサイトの脆弱性 種類別届出件数の推移（届出受付開始から2009年9月末まで）

[23] 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。



（4,708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2009年9月末まで）

前四半期と同様に今四半期も「DNS 情報の設定不備」が多く届出られました（図 2-3）。前四半期から引き続き、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 86%を占めています。

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 82%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 2009 年 9 月末までの届出の中で、修正完了したもの 2,223 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[24]。全体の 57%の届出が 30 日以内、全体の 79%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	2008/2Q まで	2008/3Q まで	2008/4Q まで	2009/1Q まで	2009/2Q まで	2009/3Q まで
77%	81%	80%	83%	80%	79%	79%

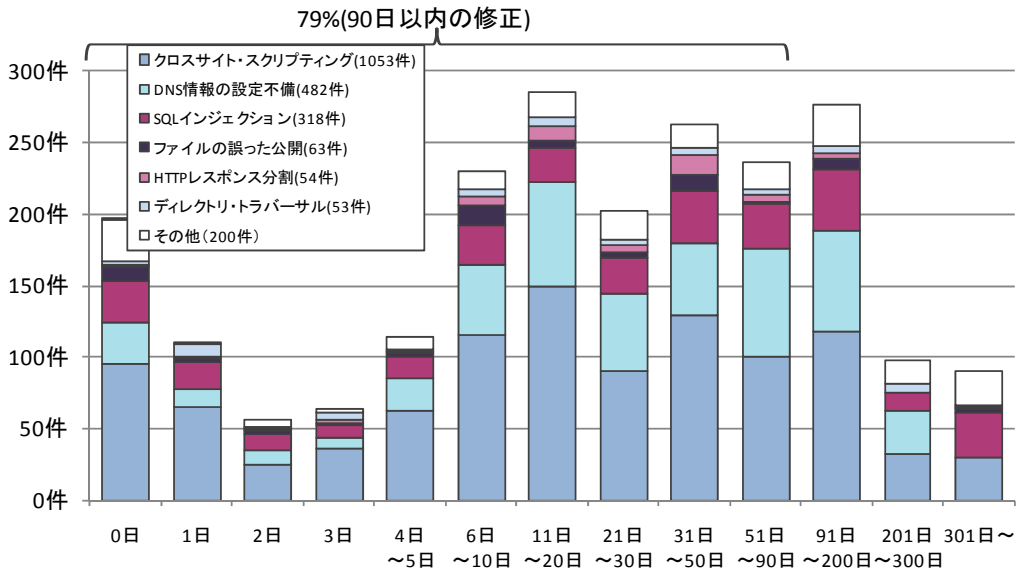


図2-5.ウェブサイトの修正に要した日数

[24] 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。

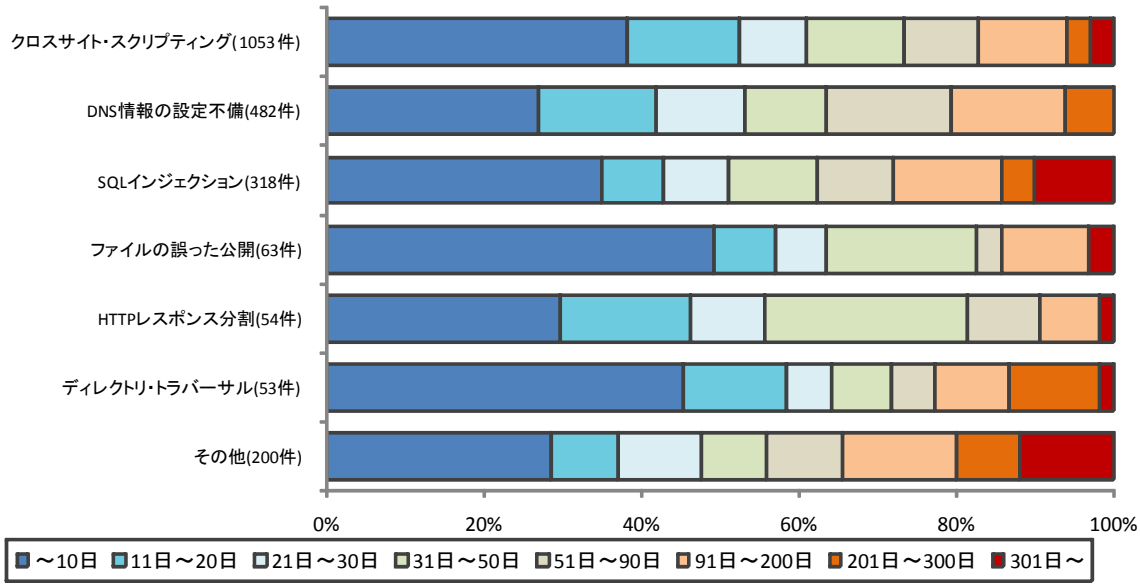


図2-6.ウェブサイトの修正に要した日数の傾向

3. 関係者への要望

脆弱性の修正を促進していくための、各関係者への要望は以下のとおりです。

(1)ウェブサイト運営者

多くのウェブサイトのソフトウェアに脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェアを利用しているかを把握し、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/

(2)製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報について、「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整を進められるよう、「製品開発者リスト」への登録を求めます（URL：http://www.jpcert.or.jp/vh/ ）。また、製品開発者自身で脆弱性を発見、修正された場合も、利用者への対策情報の周知のために JVN を活用できます。JPCERT/CC もしくは IPA への連絡を求めます。

(3)一般インターネットユーザ

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がける必要があります。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。

(4)発見者

脆弱性関連情報の適切な流通のため、届出られた脆弱性関連情報は、脆弱性が修正されるまでの期間は第三者に漏れぬよう、適切に管理することを要望します。

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

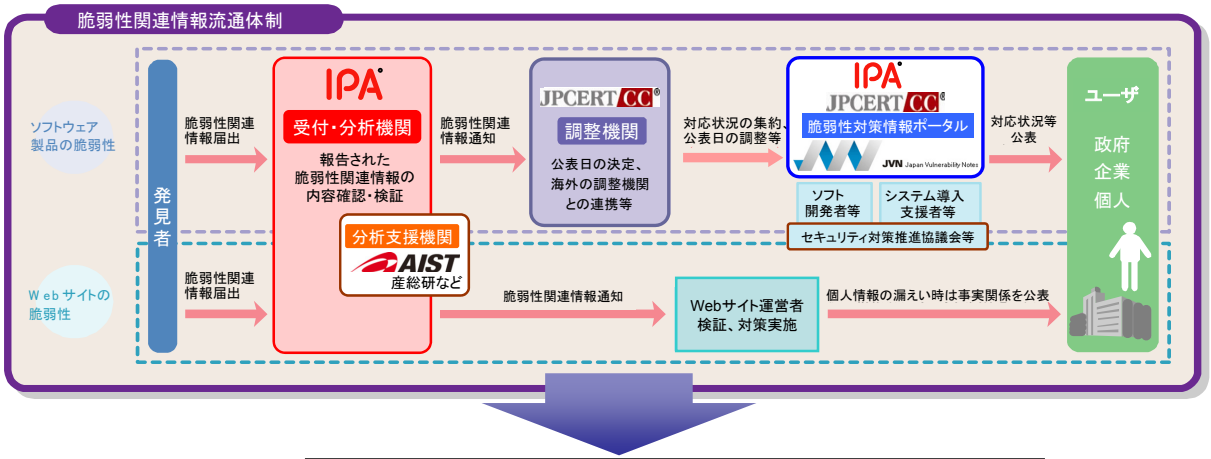
付表 2 ウェブサイト脆弱性の分類

	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