プレスリリース
2009 年 1 月 26 日
独立行政法人情報処理推進機構
有限責任中間法人 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 [2008 年第 4 四半期(10 月～12 月)]

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（有限責任中間法人 JPCERT コーディネーションセンター、代表理事：歌代 和正）は、2008 年第 4 四半期（10 月～12 月）の脆弱性関連情報の届出状況[1]をまとめました。

1.今四半期のトピックス

1.1 DNS キャッシュポイズニングの脆弱性の届出が激増

2008 年 7 月に、複数の DNS[2]サーバ製品の開発ベンダーから対策情報が公開され[3]、JPCERT/CC が注意喚起を行った[4]「DNS キャッシュポイズニングの脆弱性」に関して、「実際に運用されている DNS サーバに対策が実施されていないのでは？」という旨の届出が 9 月頃から激増しています。

図 1 は DNS キャッシュポイズニング脆弱性の各月の届出件数と 12 月末現在の対策状況です。脆弱性の届出は、対策情報の公開直後に比べて減少傾向にありますが、12 月にも 126 件の届出がありました。8 月から 12 月までの届出の累計は 792 件で、現時点で取扱い中（対策中）のものが計 674 件あります。

ウェブサイト運営者は、自組織が利用している **DNS サーバの脆弱性調査を行う**か、あるいはその **DNS サーバの管理者へ脆弱性対策状況の確認を行い、未対策の場合は対策実施を促すことが必要**です。

DNS サーバの管理者は、自組織が管理している **DNS サーバの脆弱性調査を行い、脆弱性が有る場合は、DNS サーバのパッチ適用や設定変更の早急な実施が必要**です[5]。

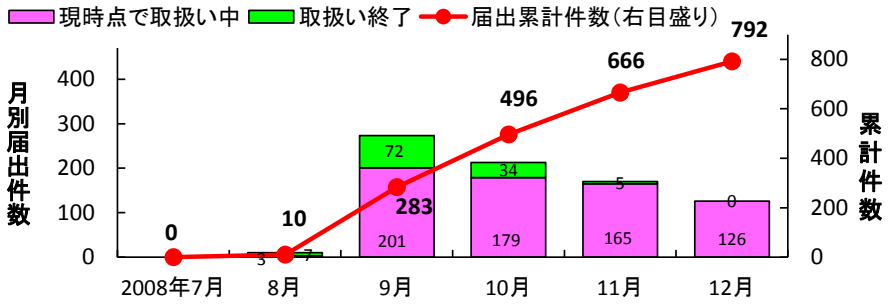


図1.DNSキャッシュポイズニング脆弱性の届出件数と対策状況 （12月末現在）

1.2 SQL インジェクションの脆弱性の届出が増加

ウェブサイトの情報の改ざんや非公開情報が公開されるなど深刻な被害が発生しており、2008 年 3 月に JPCERT/CC が注意喚起を行った[6]「SQL インジェクション攻撃」に関して、「実際に運用されているウェブサイトに SQL インジェクションの脆弱性があるのでは？」という旨の届出が増加しています。

---

[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。

[2] コンピュータがネットワークのどこに接続されているかを示す IP アドレスという数字の集まりを、www.ipa.go.jp のような人に覚えやすいドメイン表記と対応させるための情報を管理する仕組みです。

[3] 複数の DNS 実装にキャッシュポイズニングの脆弱性。http://jvn.jp/cert/JVNVU800113/index.html

[4] 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性に関する注意喚起。https://www.jpcert.or.jp/at/2008/at080014.txt

[5] 「DNS キャッシュポイズニング対策」資料を活用下さい。http://www.ipa.go.jp/security/vuln/DNS_security.html

[6] SQL インジェクションによる Web サイト改ざんに関する注意喚起。https://www.jpcert.or.jp/at/2008/at080005.txt

図 2 は SQL インジェクション脆弱性の各月の届出件数と 12 月末現在の対策状況です。3 月に多数の届出があり、8 月頃から再度、増加傾向にあります。SQL インジェクション攻撃による被害の深刻さが認識され、潜在していた脆弱性を届ける方が増加してきているものと考えています。2008 年の 1 月から 12 月までの届出の累計は 263 件で、現時点で取扱い中（対策中）のものが計 202 件あります。

ウェブサイト管理者は、ウェブサーバのアクセスログ調査[7]およびウェブサイトの脆弱性検査等を行い、脆弱性が有る場合は、ウェブサイトの SQL インジェクション対策の早急な実施が必要です[8]。

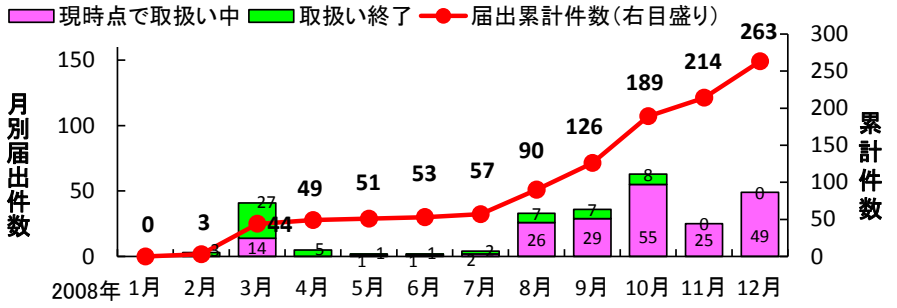


図2.SQLインジェクション脆弱性の届出件数と対策状況

1.3 脆弱性対策情報ポータルサイト JVN の CVE 互換を宣言しました

共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）[9]は、個別製品中の脆弱性を対象として、米国 MITRE 社が採番している識別子です。

MITRE 社では、CERT/CC や HP、IBM、OSVDB、Red Hat、Symantec など 80 を超える主要な脆弱性情報サイトと連携して、脆弱性情報の収集と、重複のない採番に努めています。

IPA と JPCERT/CC が共同で運営している JVN（Japan Vulnerability Notes）[10]も、MITRE 社と連携して CVE 採番の枠組みに参加するため、JVN で公表する脆弱性に対する CVE の割り当てを申請することとし、**2008 年 10 月からは MITRE 社が公表している「CVE 情報源サイト」の一つとして公示されるようになりました[11]。**さらに **2008 年 12 月には、JVN としての連携の意思を明確に示すため、「CVE 互換宣言」を行いました[12]。**

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。

1.4 今四半期の届出状況

2008 年第 4 四半期（2008 年 10 月 1 日から 12 月 31 日まで）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 **60** 件、ウェブアプリケーション（ウェブサイト）に関するもの **1,430** 件、合計 **1,490** 件でした。

表 1. 2008 年第 4 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	**60** 件	**861** 件
ウェブサイト	**1,430** 件	**3,514** 件
計	**1,490** 件	**4,375** 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 **861** 件、ウェブサイトに関するもの **3,514** 件、合計 **4,375** 件となりました。

---

[7] 「SQL インジェクション検出ツール iLogScanner」を活用下さい。http://www.ipa.go.jp/security/vuln/iLogScanner/

[8] 「安全なウェブサイトの作り方」を活用下さい。http://www.ipa.go.jp/security/vuln/websecurity.html

[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・運営しています。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

[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

ウェブサイトに関する届出が全体の約 5 分の 4 を占めています（表 1）。

届出が年々増加しており、届出受付開始（2004 年 7 月 8 日）から各四半期末までの業務日 1 日あたりの届出件数が、今四半期で **4.00** 件となりました。**届出受付開始から 4 年間（2004 年 3Q～2008 年 2Q）で累計件数が 2,300 件に達しましたが、その後、半年間（2008 年 3Q～4Q）で 4,300 件に達しました（図 3）。**これは、2008 年第 3 四半期ごろから DNS キャッシュポイズニング、SQL インジェクション、クロスサイト・スクリプティングの脆弱性の届出が激増しているためです。

就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

2006/1Q	2007/1Q	2007/2Q	2007/3Q	2007/4Q	2008/1Q	2008/2Q	2008/3Q	2008/4Q
1.61	1.95	1.98	2.03	2.05	2.24	2.38	2.79	4.00

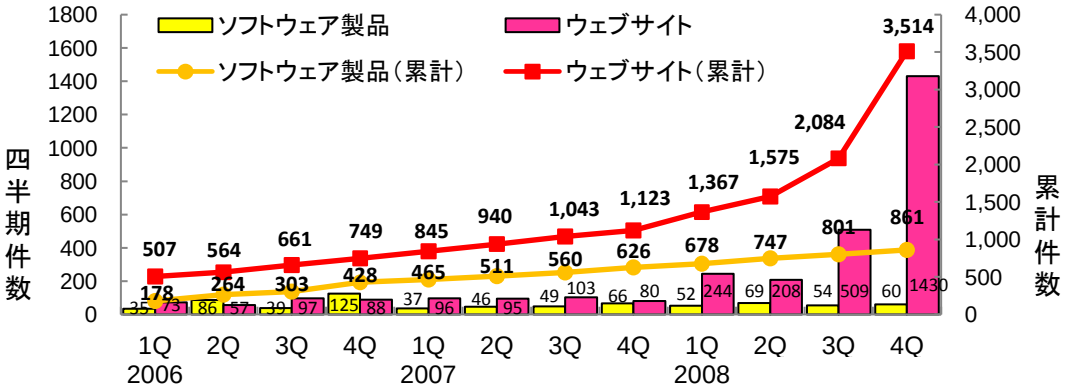


図3.脆弱性関連情報の届出件数の四半期別推移

2.ソフトウェア製品の脆弱性の処理状況

2008 年第 4 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は **22** 件でした。製品開発者からの届出のうち JVN で公表せず製品開発者が個別対応を行ったものは **0** 件、製品開発者が脆弱性ではないと判断したものは **1** 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 **16** 件でした。これらの取扱いを終了したものの合計は **39** 件（累計 **504** 件）です（表 2）。

表 2. ソフトウェア製品の脆弱性の終了件数

分類		件数	累計件数
修正完了	公表済み	**22** 件	**321** 件
	個別対応	**0** 件	**16** 件
脆弱性ではない		**1** 件	**35** 件
不受理		**16** 件	**132** 件
合計		**39** 件	**504** 件

この他、海外の CSIRT[13]から JPCERT/CC が連絡を受けた **17** 件（累計 **392** 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 4 に示します。

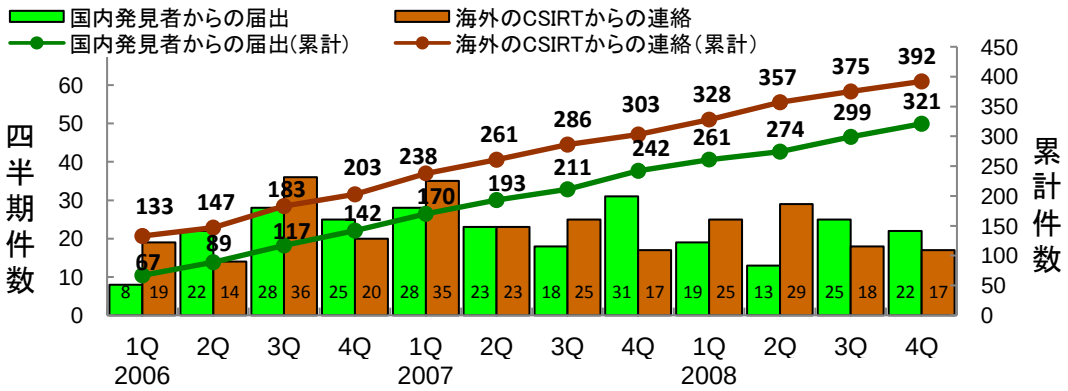


図4.ソフトウェア製品の脆弱性対策情報の公表件数

[13] 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。

2008 年第 4 四半期において、JVN で対策情報を公表した主な脆弱性は、以下のとおりです。

(1) 「EC-CUBE」における SQL インジェクションの脆弱性[14]

株式会社ロックオンが提供するオープンソースのショッピングサイト構築システムの「EC-CUBE」には、データベースと通信する際の処理に問題があり、SQL インジェクションの脆弱性が存在しました。

この弱点が悪用されると、「EC-CUBE」の管理者権限が外部の第三者に取得され、「EC-CUBE」上に登録されている個人情報が漏えいする可能性があり、10 月 1 日および 11 月 6 日に JVN で対策情報を公表しました。

この脆弱性情報は、製品開発者自身から IPA に届出があり、JPCERT/CC が製品開発者と調整を行ない公表したものです。今後も、**JVN が製品開発者によって、脆弱性対策情報の利用者への周知手段として活用されることを期待します。**

(2) アイ・オー・データ製「HDL-F シリーズ」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[15]

株式会社アイ・オー・データ機器が提供する、LAN 接続型ハードディスク「HDL-F シリーズ」のウェブ管理画面には、クロスサイト・リクエスト・フォージェリ（CSRF）の脆弱性が存在しました。悪意あるページを読み込んだ利用者が、ウェブ管理画面で意図しない操作をさせられてしまう可能性があり、11 月 26 日に JVN で対策情報を公表しました。

3.ウェブサイトの脆弱性の処理状況

2008 年第 4 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 **201** 件、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 **5** 件、ウェブサイト運営者と連絡が不可能なものが **0** 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** 件でした。これらの取扱いを終了したものの合計は **221** 件（累計 **1,607** 件）です（表 3）。

表 3. ウェブサイトの脆弱性の終了件数

分類	件数	累計件数
修正完了	**201** 件	**1334** 件
脆弱性ではない	**5** 件	**167** 件
連絡不可能	**0** 件	**7** 件
不受理	**15** 件	**99** 件
合計	**221** 件	**1,607** 件

これらのうち、修正完了件数の期別推移を図 5 に示します。

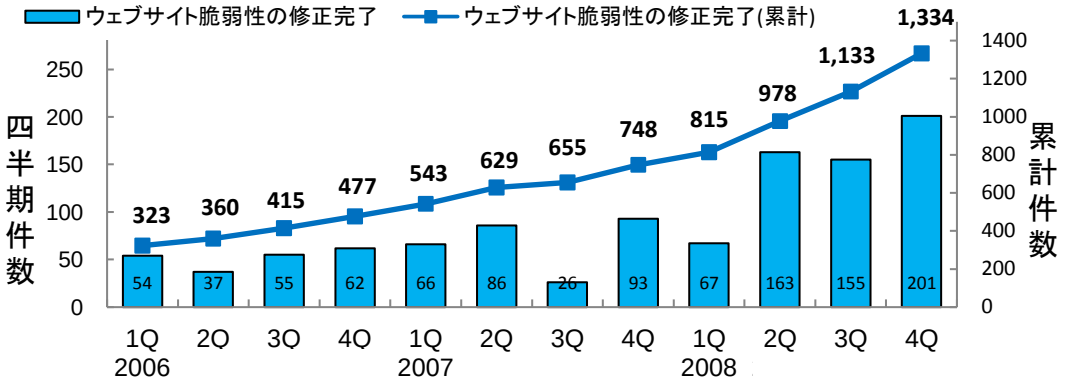


図5.ウェブサイトの脆弱性の修正完了件数

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のあった対象ウェブサイトの運営主体別内訳は、地方公共団体が 45%、企業

[14] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.5、別紙 P.4 表 1-2 項番 1 と項番 2 を参照下さい。
[15] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0、別紙 P.4 表 1-2 項番 3 を参照下さい。

合計が 36%、政府機関が 7%、教育・学術機関が 5%、団体（協会・社団法人）が 5%、個人が 1%などとなっています（図 6）。

また、今四半期に届出のあったウェブサイトの脆弱性の種類の内訳は、クロスサイト・スクリプティングが 46%、DNS 情報の設定不備（DNS キャッシュポイズニングの脆弱性）が 36%、SQL インジェクションが 10%、HTTPS の不適切な利用が 3%、HTTP レスポンス分割が 3%などとなっています（図 7）。

広く知れ渡っている脆弱性が数多く届出られており、ウェブサイト開発者は既知の脆弱性を認識し、ウェブサイトの企画・設計段階からのセキュリティの考慮が必要です。

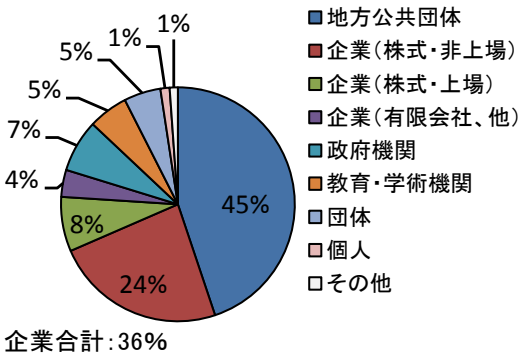


図6.ウェブサイトの運営主体（2008年第4四半期）

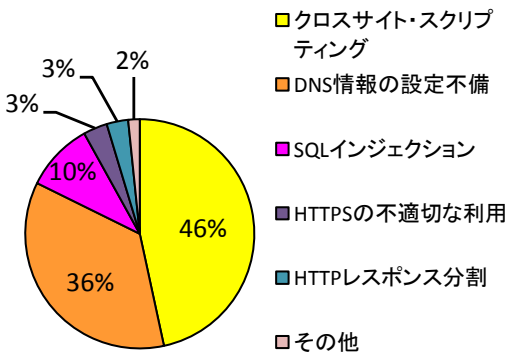


図7.ウェブサイトの脆弱性の種類（2008年第4四半期）

3.2 ウェブサイトの脆弱性で 90 日以上対策が未完了のものは 258 件

IPA は、ウェブサイト運営者から脆弱性対策の返信がない場合、脆弱性が攻撃された場合の脅威を丁寧に解説するなど、1～2 カ月毎にメールや郵送手段などで脆弱性対策を促しています。

図 8 はウェブサイトの脆弱性で 90 日以上対策が完了していないものの経過日数毎の件数を示しています。経過日数が 90 日から 199 日に達したものは 117 件、200 日から 299 日のものは 60 件などとなっており、これらの合計は **258** 件（前四半期は **179** 件）となりました。前四半期のものは **38** 件減少しましたが、今四半期で新たに **117** 件が 90 日以上となったため、**79** 件が増加しています。

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、早期に対策を講じる必要があります。**

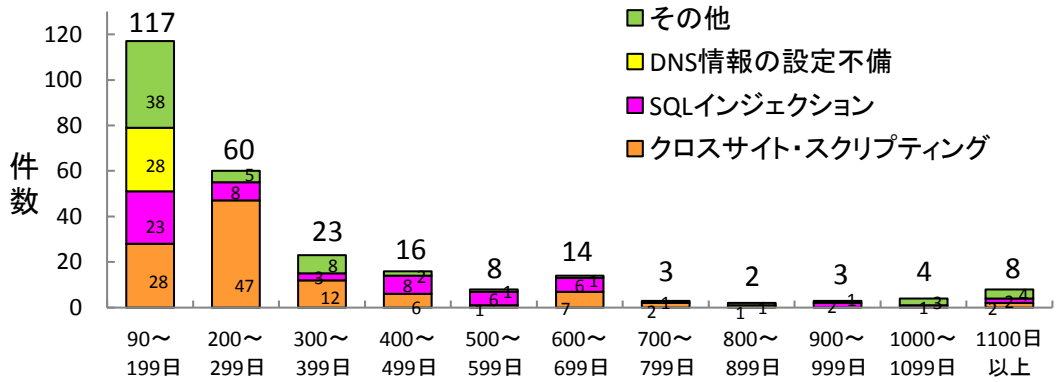


図8. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

4. 脆弱性対策を完了したウェブサイト運営者からのアンケート集計結果

IPA から脆弱性の通知を行い、脆弱性対策を完了したウェブサイト運営者へ、セキュリティ意識などのアンケートを実施しています。昨年 7 月から 210 件（約 93%の回収率）の回答がありました。

図 9 の棒グラフは、発見された脆弱性が「クロスサイト・スクリプティング」と「SQL インジェクシ

ョン」であったと回答のあった 70 件に関して、その件数を、ウェブサイトを開発した時期別に示しています。また、折れ線グラフは、そのウェブサイト開発時に「セキュリティの意識があった」と回答のあった割合を示しています。2006 年以前は 30%程度だった「セキュリティ意識」は、2007-2008 年に 50%となりましたが、まだ低い状況です。

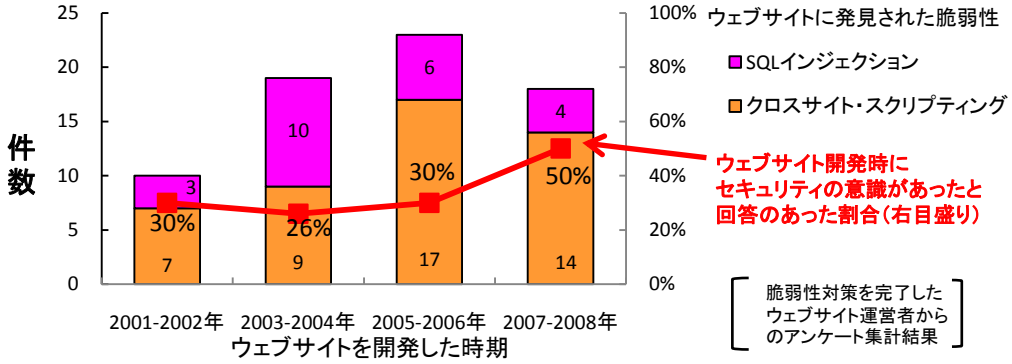


図9.ウェブサイトに発見された脆弱性の種類とセキュリティ意識の推移

図 10 の棒グラフは、脆弱性対策のアンケートに回答があったウェブサイトに関して、集客性、デザイン性、利用者の利便性、運営・管理の利便性、セキュリティのどの項目を意識して開発したか（複数回答有り）回答があった 106 件を、そのウェブサイトの運営者主体別に示しています。また、赤まる印は、そのウェブサイトを、「セキュリティ対策を行って開発した」と回答があった割合を示しています。

脆弱性対策後のアンケートに回答があったウェブサイトのうち、非上場会社、団体（協会・社団法人）など、中小規模のウェブサイトにおいて、開発時に「セキュリティ対策を行っていない」と回答がありました。**ウェブサイト開発時から適切なセキュリティを考慮した実装を行う必要があります。**

また、脆弱性対策後のアンケートに回答があったウェブサイトのうち、上場会社、地方公共団体、政府機関などは、ウェブサイト開発時に 8 割近くが「セキュリティ対策を行った」と回答があったにもかかわらず、脆弱性が発見されています。**脆弱性は日々新たに発見されています。セキュリティ対策は開発時のみに行うのではなく、定期的な脆弱性検査を行う必要があります。**

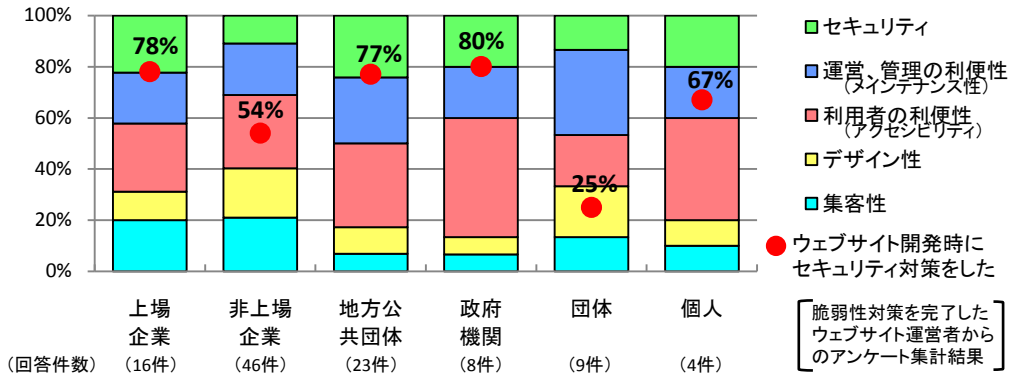


図10.ウェブサイト運営者主体別の意識と開発時のセキュリティ対策の有無

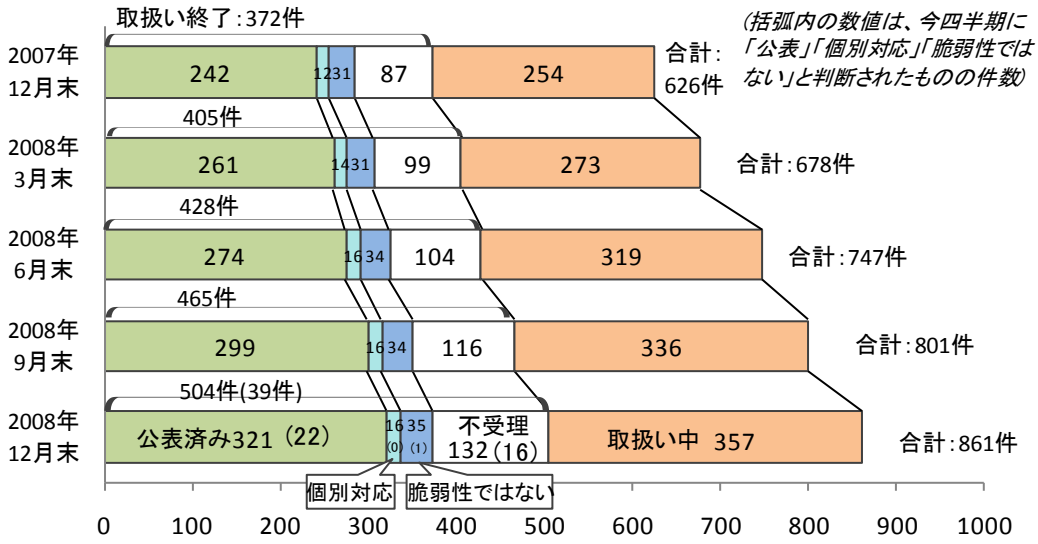
■ 本件に関するお問い合わせ先
IPA セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
JPCERT/CC 情報流通対策グループ 古田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: office@jpcert.or.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp
JPCERT/CC 経営企画室 広報 江田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: pr@jpcert.or.jp

別紙

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、**22** 件（累計 **321** 件）です。また、「不受理」としたものは **16** 件（累計 **132** 件）です。



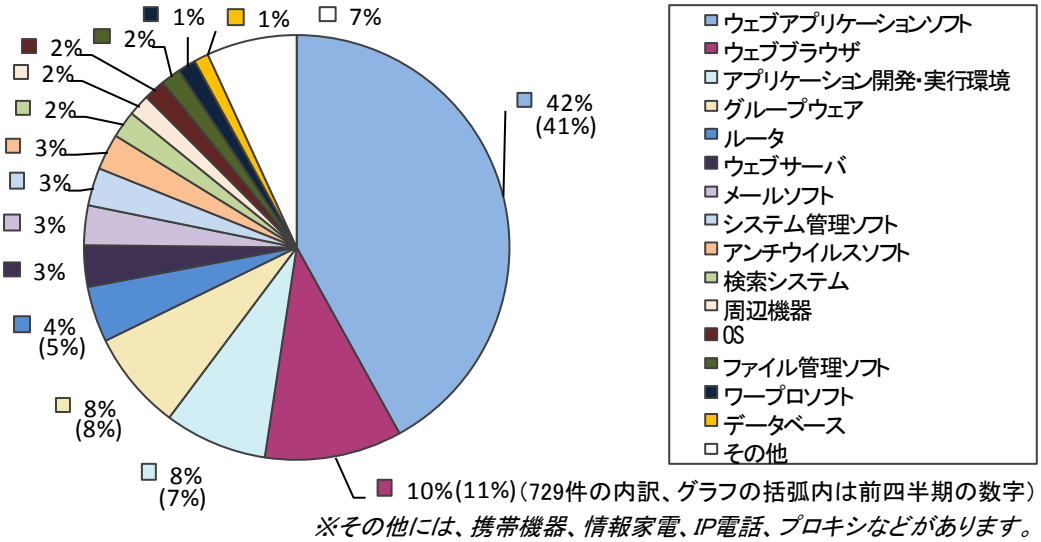
公表済み:	JVN で脆弱性への対応状況を公表したもの
個別対応:	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない:	製品開発者により脆弱性ではないと判断されたもの
不受理:	告示で定める届出の対象に該当しないもの
取扱い中:	製品開発者が調査、対応中のもの

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 **861** 件のうち、不受理のものを除いた **729** 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。



(729件の内訳、グラフの括弧内は前四半期の数字)

※その他には、携帯機器、情報家電、IP電話、プロキシなどがあります。

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2008年12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 **861** 件のうち、不受理のものを除いた **729** 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。2005 年第 3 四半期以降、オープンソースソフトウェアの届出が今四半期も前四半期と同じ **20** 件の届出がありました。

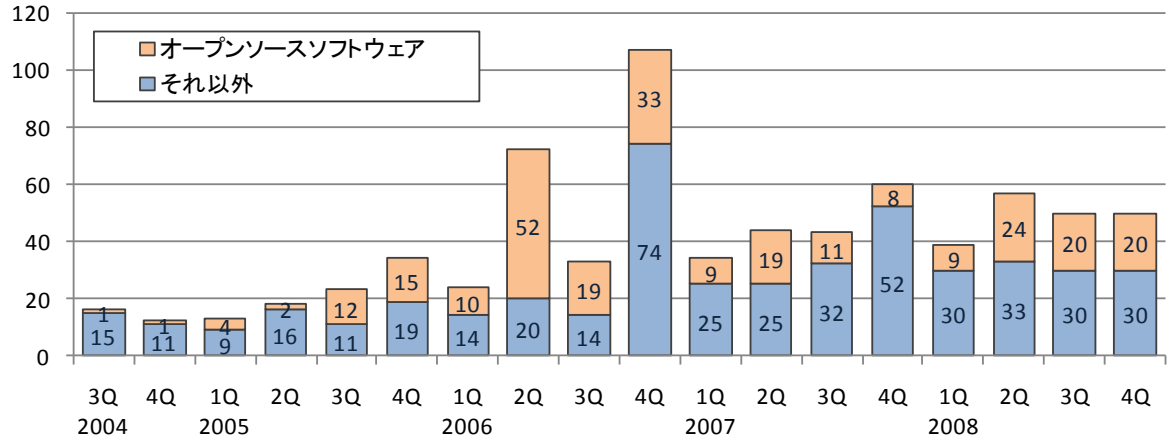
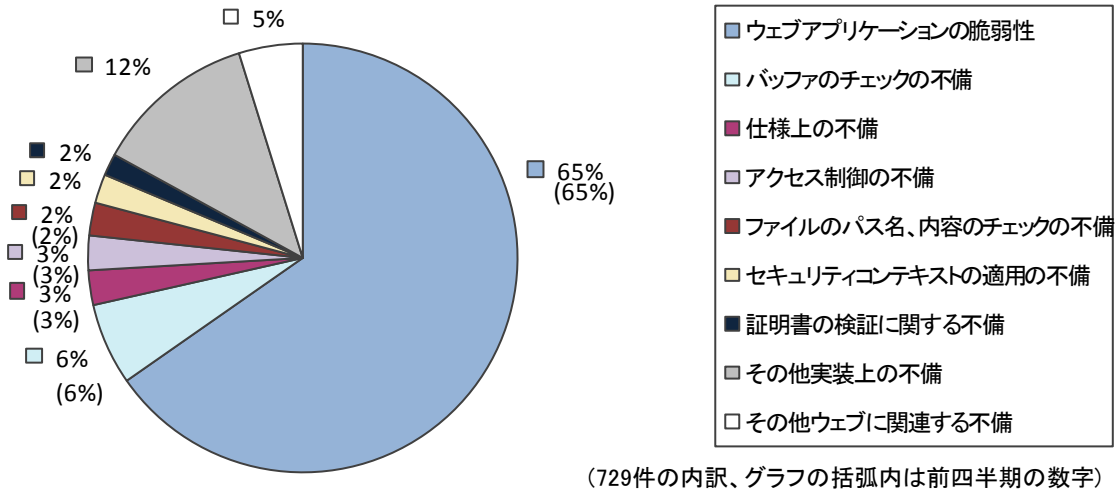


図1-3.オープンソースソフトウェアの脆弱性の届出件数　（729件の内訳）

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 **861** 件のうち、不受理のものを除いた **729** 件の原因別の内訳を図 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で、この傾向は図 1-5 に示すように、届出受付開始から続いています。



（729件の内訳、グラフの括弧内は前四半期の数字）

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2008年12月末まで）

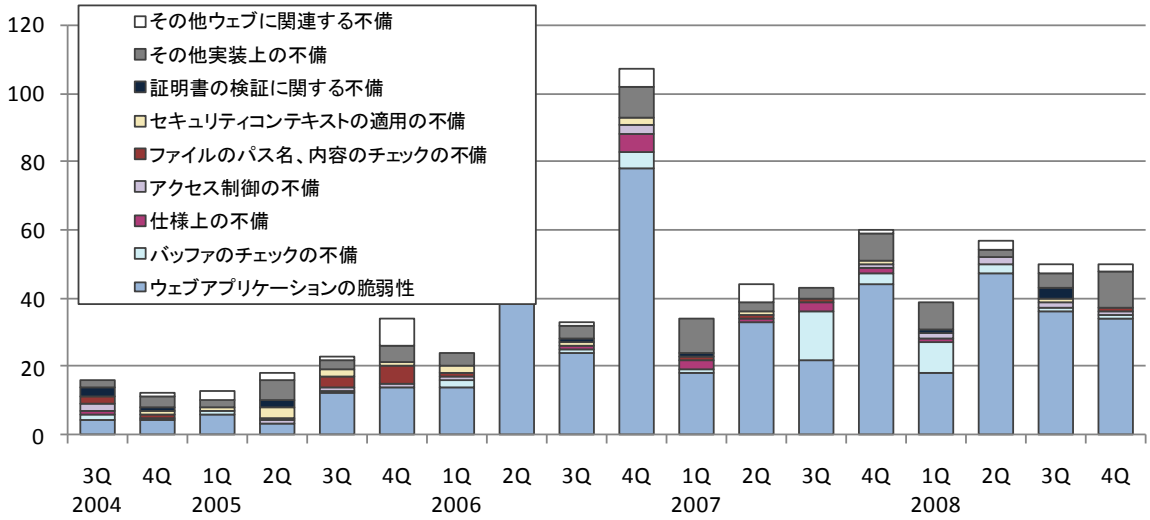
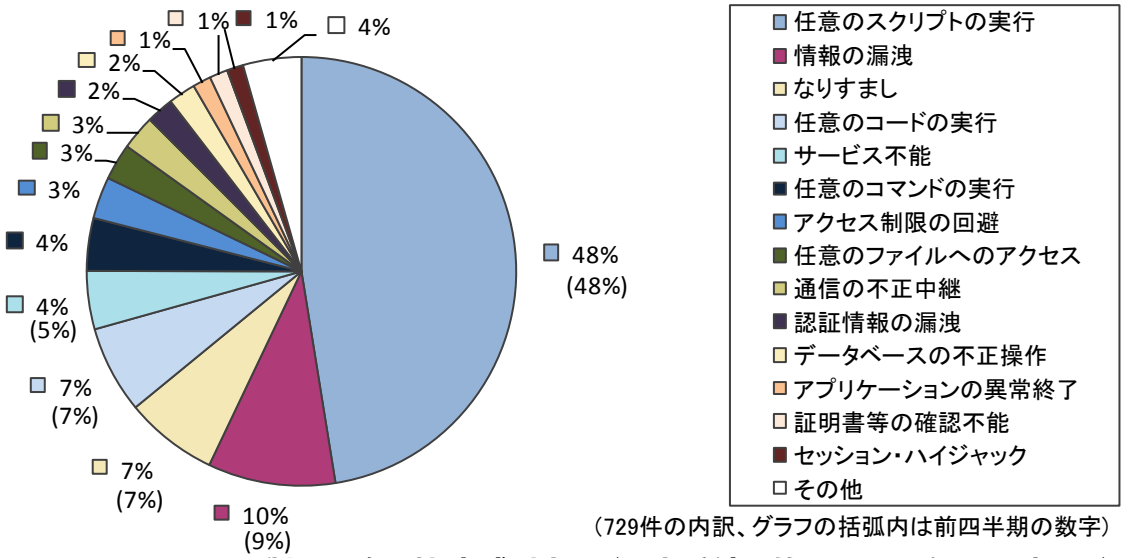


図1-5. ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2008年12月末まで）



（729件の内訳、グラフの括弧内は前四半期の数字）

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2008年12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[16] 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	22 件	321 件
②	海外 CSIRT 等と連携して公表したもの	17 件	392 件
	計	39 件	713 件

[16] 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 2008 年 12 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 32%であり、公表するまでに要した日数は 2008 年第 2 四半期から変わらずに推移しています。製品開発者は脆弱性への早急な対応をお願いします。

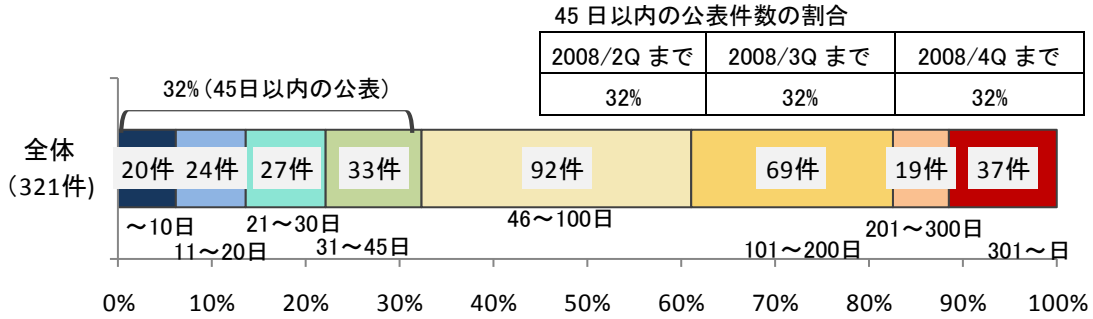


図1-7. ソフトウェア製品の脆弱性公表日数

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て開発者、開発コミュニティに通知し公表したものが 13 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 4 件（表 1-2 の*2）、組込みソフトウェア製品の脆弱性が 1 件（表 1-2 の*3）ありました。

表 1-2.2008 年第 4 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.				
1 (*1) (*2)	「EC-CUBE」における SQL インジェクションの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」には、利用者から入力された内容を元に 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。	2008 年 10 月 1 日	7.5
2 (*1) (*2)	「EC-CUBE」における SQL インジェクションの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」には、利用者から入力された内容を元に 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。	2008 年 11 月 6 日	7.5
3 (*3)	アイ・オー・データ製「HDL-F シリーズ」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	LAN 接続型ハードディスクである HDL-F シリーズのウェブ管理画面には、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、ウェブ管理画面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、ハードディスク上のデータが削除されたり、設定が変更される可能性がありました。	2008 年 11 月 26 日	7.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
4 (*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。	2008 年 10 月 1 日	4.3
5 (*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。	2008 年 10 月 1 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
6 (*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。	2008 年 10 月 1 日	4.3
7 (*1)	「Nucleus」EUC-JP 日本語版におけるクロスサイト・スクリプティングの脆弱性	コンテンツ管理システム「Nucleus」EUC-JP 日本語版には、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。	2008 年 10 月 6 日	4.3
8	「hisa_cart」における情報漏洩の脆弱性	XOOPS 用のショッピングカートモジュール「hisa_cart」には、利用者に関する情報が漏洩してしまう脆弱性がありました。このため、遠隔の第三者により、利用者の情報等が取得される可能性がありました。	2008 年 10 月 17 日	5.0
9 (*1)	「Movable Type」におけるクロスサイト・スクリプティングの脆弱性	ウェブログ作成管理システム「Movable Type」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、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。	2008 年 10 月 17 日	4.0
10 (*1)	「Blosxom」におけるクロスサイト・スクリプティングの脆弱性	ウェブログ作成管理システム「Blosxom」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。	2008 年 10 月 20 日	4.3
11 (*1)	「Snoopy」における OS コマンド・インジェクションの脆弱性	PHP ライブラリである「Snoopy」には、利用者からの入力内容の処理に問題がありました。このため、Snoopy を設置し実行可能に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。	2008 年 10 月 28 日	5.1
12 (*2)	「sISAPILocation」における HTTP ヘッダ書き換え回避の脆弱性	IIS 上で動作する ISAPI フィルタである「sISAPILocation」には、HTTP ヘッダの書き換え機能が回避される脆弱性がありました。このため、sISAPILocation で文字コードの指定や Cookie の secure フラグなどの設定を行っている場合、それらの設定が回避される可能性がありました。	2008 年 11 月 6 日	4.3
13	CGI RESCUE 製「簡易 BBS2000」におけるディレクトリ・トラバーサルの脆弱性	電子掲示板スクリプト「簡易 BBS2000」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、簡易 BBS2000 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。	2008 年 11 月 21 日	6.4
14	「Movable Type Enterprise」におけるクロスサイト・スクリプティングの脆弱性	ウェブログ作成管理システム「Movable Type Enterprise」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。	2008 年 12 月 3 日	4.3
15	futomi's CGI Cafe 製「高機能アクセス解析 CGI」におけるセッション ID が推測可能な脆弱性	アクセスログ解析ソフト「高機能アクセス解析 CGI」には、セッション ID が推測可能である脆弱性がありました。このため、遠隔の第三者により、高機能アクセス解析 CGI の管理者になりすまされる可能性がありました。	2008 年 12 月 12 日	5.8
16 (*1)	「Mayaa」におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーション開発支援ソフト「Mayaa」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。	2008 年 12 月 25 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
17 (*1)	「BlackJumboDog」における認証回避の脆弱性	簡易サーバ「BlackJumboDog」には、認証回避が可能な脆弱性がありました。このため、遠隔の第三者によって、BlackJumboDog の認証機能が回避され、結果として情報が漏えいする可能性がありました。	2008 年 12 月 25 日	5.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
18 (*1)	「Apache Tomcat」において権限のないクライアントからのリクエストが実行されてしまう脆弱性	The Apache Software Foundation が提供する「Apache Tomcat」には、権限のないクライアントからのリクエストが実行されてしまう脆弱性がありました。このため、情報が漏えいする可能性がありました。	2008 年 10 月 10 日	2.6
19	「Internet Explorer」における CDO によるダウンロードのダイアログボックス回避の脆弱性	「Internet Explorer」には、CDO によりダウンロードのダイアログボックスを回避可能な問題がありました。このため、ダウンロードのダイアログボックスが表示されないため、意図せず任意のスクリプトを実行される可能性がありました。	2008 年 10 月 20 日	2.6
20 (*2)	「MyNETS」におけるクロスサイト・スクリプティングの脆弱性	SNS ソフト「MyNETS」には、クロスサイト・スクリプティングの脆弱性がありました。このため、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。	2008 年 10 月 20 日	3.5
21	ガンホー製「LoadPrgAx」において任意の Java プログラムが実行される脆弱性	ゲームを起動するための ActiveX コトロール「LoadPrgAx」には、任意の Java プログラムが実行される脆弱性がありました。このため、細工された HTML ドキュメント (ウェブページや HTML 形式のメール) を利用者が閲覧した場合、利用者の PC 内にある任意の Java プログラムを実行される可能性がありました。	2008 年 11 月 17 日	2.6
22 (*1)	「PHP」におけるクロスサイト・スクリプティングの脆弱性	スクリプト言語の実行環境「PHP」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。	2008 年 12 月 19 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

JPCERT/CC が海外 CSIRT 等と連携して公表した脆弱性 17 件には、通常の脆弱性情報 7 件（表 1-3）と、対応に緊急を要する Technical Cyber Security Alert（表 1-4）の 9 件と、CPNI からの情報 1 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[17]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	IPv6 実装における Forward Information Base のアップデートに関する問題	複数製品開発者へ通知
2	Automated Solutions Modbus Slave ActiveX Control における脆弱性	注意喚起として掲載
3	libspf2 の DNS TXT レコード解析処理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
4	DATAC RealWin 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
5	Microsoft Internet Explorer のデータバインディング処理における脆弱性	緊急案件として掲載
6	Microsoft ワードパッドのテキストコンバータに任意のコードが実行可能な脆弱性	注意喚起として掲載
7	Microsoft SQL Server の sp_replwritetovarbin 拡張ストアド プロシージャの処理における脆弱性	注意喚起として掲載

表 1-4.米国 US-CERT[18]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 Windows Server サービスにバッファオーバーフローの脆弱性
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	Microsoft 製品における複数の脆弱性に対するアップデート
5	Mozilla 製品における複数の脆弱性に対するアップデート
6	Java 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
8	Apple 製品における複数の脆弱性に対するアップデート
9	Microsoft Internet Explorer のデータバインディング処理における脆弱性

表 1-5.英国 CPNI[19]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	SSH 通信において一部データが漏えいする可能性

[17] 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。
[18] United States Computer Emergency Readiness Team。米国の政府系 CSIRT。
[19] Centre for the Protection of National Infrastructure。イギリス政府機関（国家インフラ保護センター）。

2. ウェブサイトの脆弱性の処理状況の詳細

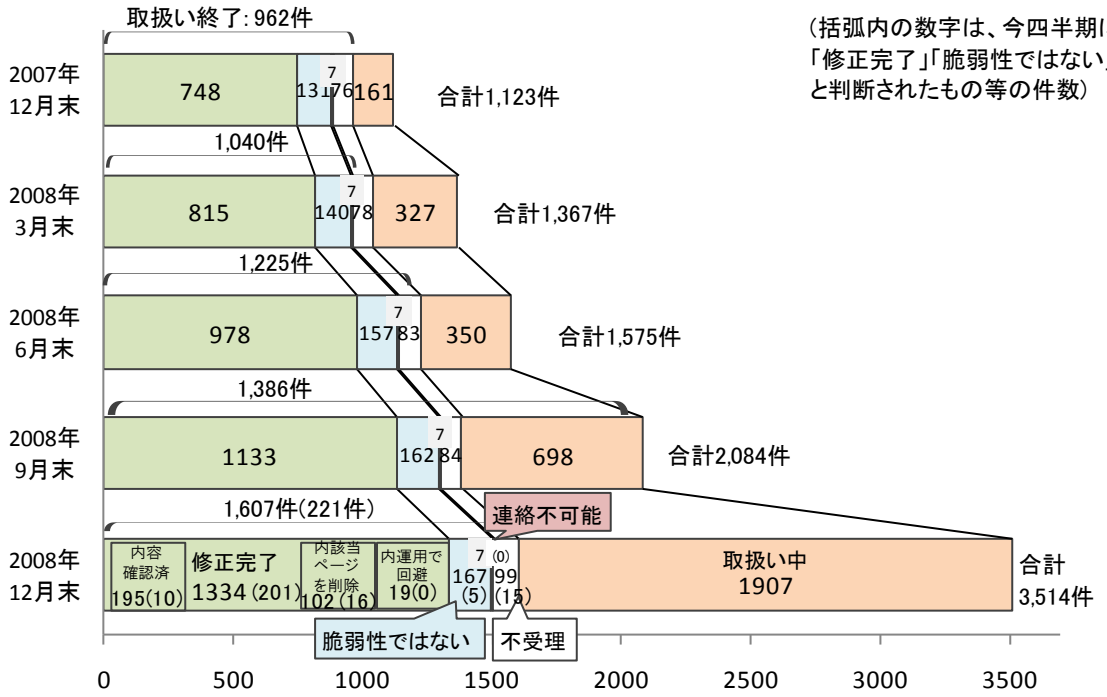
2.1 ウェブサイトの脆弱性の処理状況

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 **221** 件（累計 **1,607** 件）でした。このうち、「修正完了」したものは **201** 件（累計 **1,334** 件）、ウェブサイト運営者により「脆弱性ではない」と判断されたものは **5** 件（累計 **167** 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「取扱い不可能」なものは **0** 件(累計 **7** 件)です。「不受理」としたものは **15** 件（累計 **99** 件）でした。

取扱いを終了した累計 **1,607** 件のうち、「連絡不可能」「不受理」を除く累計 **1,501** 件（**93**%）は、指摘した点が解消されていることが、ウェブサイト運営者により報告されています。

「修正完了」したものうちのウェブサイト運営者からの依頼を受け、当該脆弱性が適切に修正されたかどうかを IPA が確認したものは **10** 件（累計 **195** 件）、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 **16** 件（累計 **102** 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 **19** 件）でした。

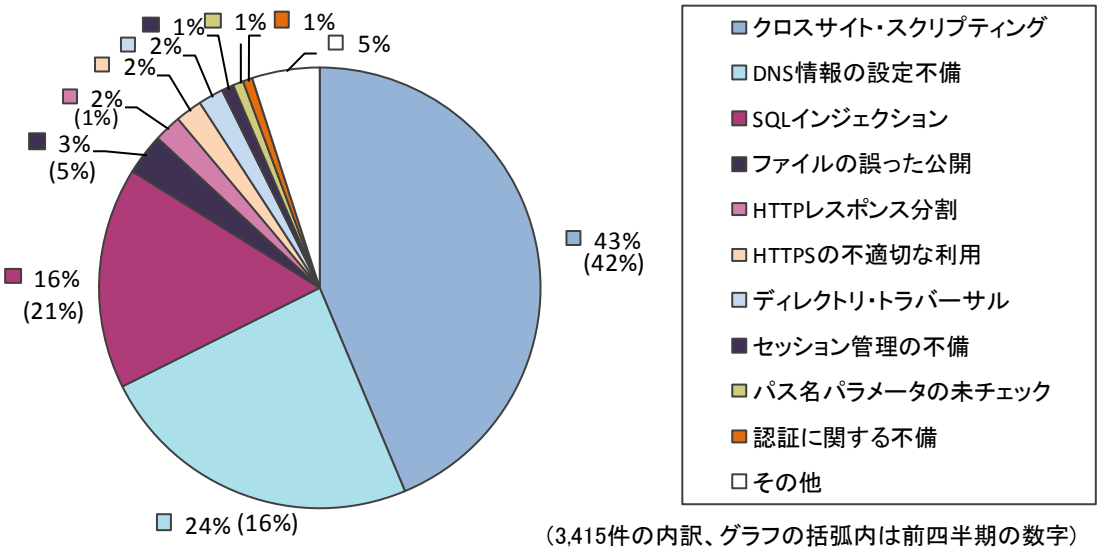


修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
確認済	：	修正完了のうち、IPA が修正を確認したもの
当該ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
運用で回避	：	修正完了のうち、運用により被害を回避しているもの
脆弱性ではない	：	ウェブサイト運営者により脆弱性はないと判断されたもの
連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
不受理	：	告示で定める届出の対象に該当しないもの
取扱い中	：	ウェブサイト運営者が調査、対応中のもの

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**3,514**件のうち、不受理のものを除いた**3,415**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[20]。



（3,415件の内訳、グラフの括弧内は前四半期の数字）

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2008年12月末まで）

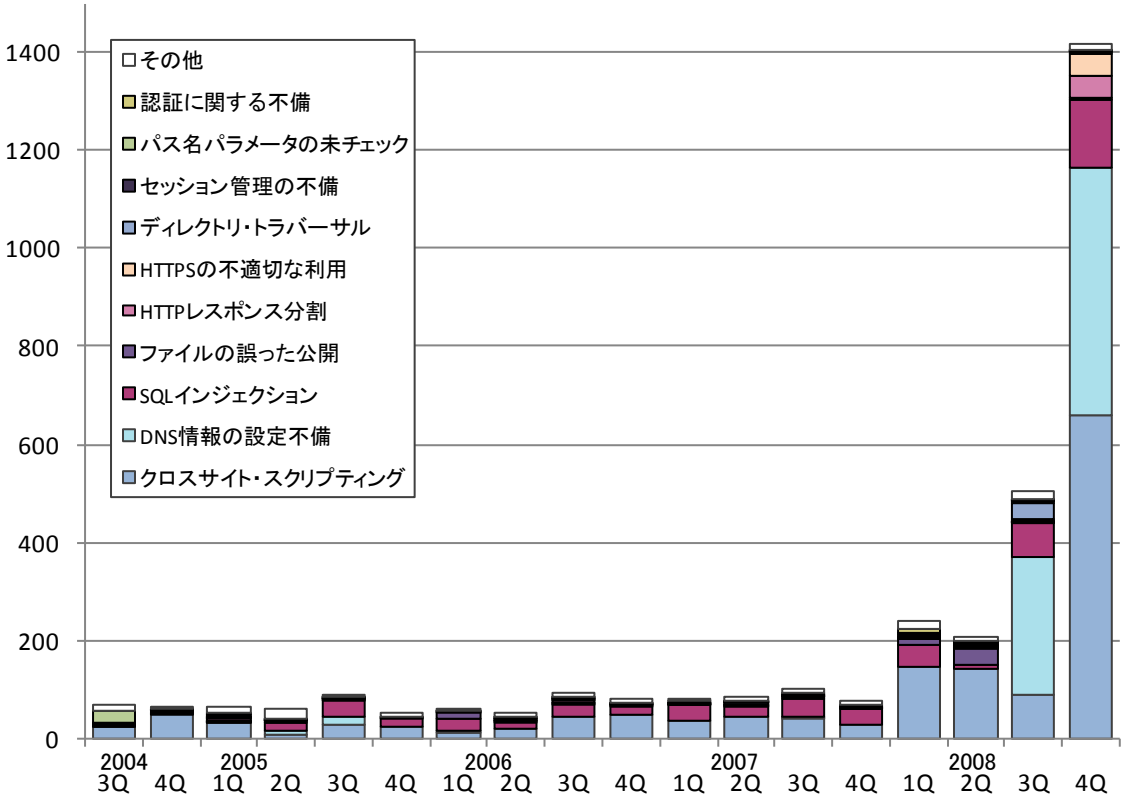
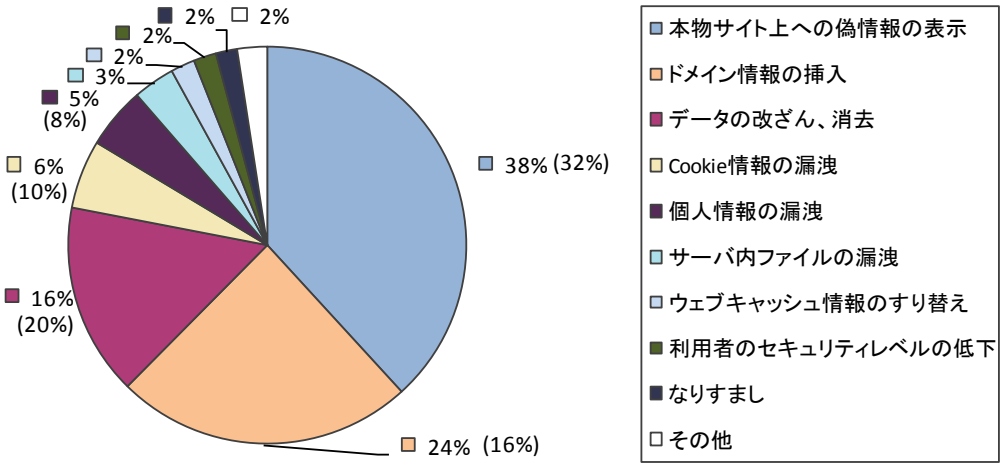


図2-3.ウェブサイトの脆弱性 種類別件数の推移（届出受付開始から2008年12月末まで）

[20] 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。



（3,415件の内訳、グラフの括弧内は前四半期の数字）

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2008年12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）。届出受付開始から脆弱性の種類の割合は 1 位「クロスサイト・スクリプティング」、2 位「SQL インジェクション」でしたが、今四半期ではじめて「DNS 情報の設定不備」が「SQL インジェクション」の割合を上回りました（図 2-2）。

また「クロスサイト・スクリプティング」や「DNS 情報の設定不備」や「SQL インジェクション」の脅威である、「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 84%をしめています（図 2-4）。

ウェブサイト運営者は、引き続き脆弱性を作りこまないように注意してください。

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 2008 年 12 月末までの届出の中で、実際にウェブアプリケーションを修正したものについて、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。全体の 60%の届出が 30 日以内、全体の 83%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
77%	81%	80%	83%

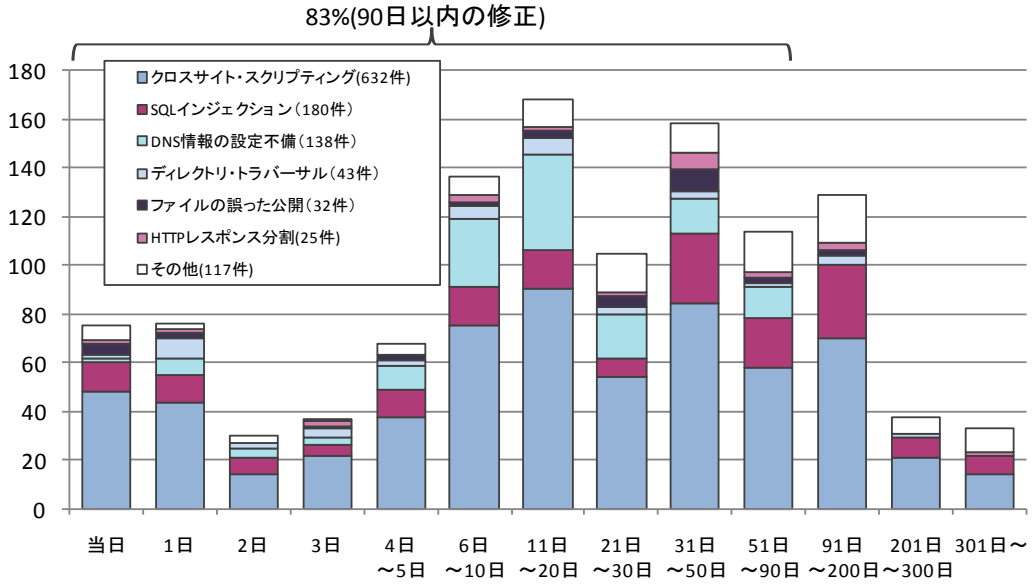


図2-5.ウェブサイトの修正に要した日数

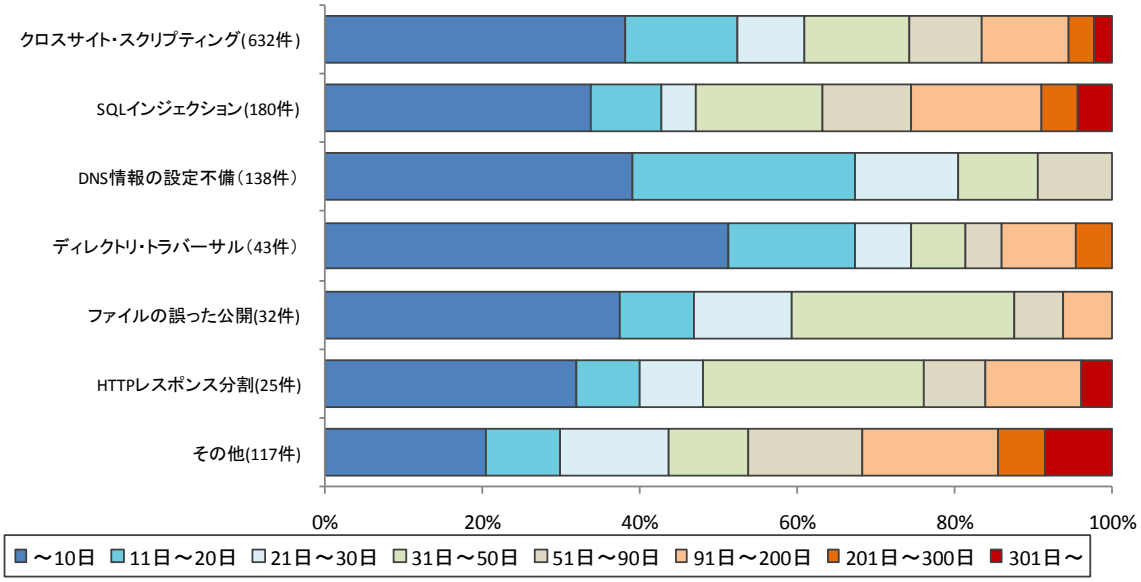


図2-6.ウェブサイトの修正に要した日数の傾向

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ていただくことが必要です。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、適切に管理され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。プロトコル上の不備がある場合、ここに含まれる	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

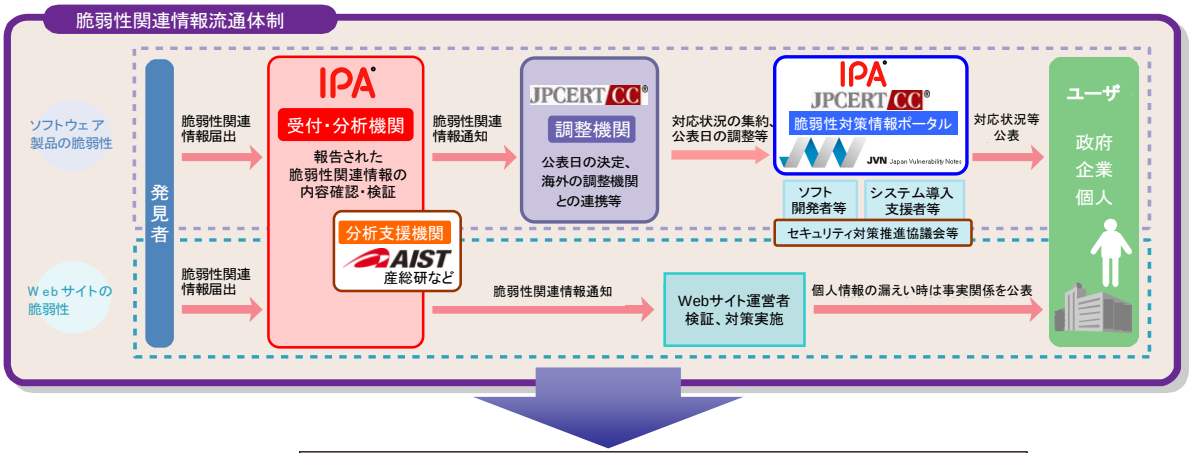
付表 2 ウェブサイト脆弱性の分類

	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：有限責任中間法人 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