プレスリリース
2010 年 1 月 21 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 4 四半期（10 月～12 月）]

～ 2004 年 7 月の届出受付開始から 5 年半が経過し、修正完了件数の累計が 3,000 件に達しました ～

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 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。

2004 年 7 月の届出受付開始から 5 年半が経過し、脆弱性関連情報の届出に関して、製品開発者やウェブサイト運営者が修正を完了したものの累計が 3,054 件となりました。このうち、1,000 件は 2009 年の 1 年間に修正を完了しています。修正完了件数が年々増加しており、制度として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。

## (1)修正完了件数の累計が 3,000 件に達しました

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、2009 年第 4 四半期に JVN[2]で対策情報を公表したものが 16 件（累計 400 件）でした。

ウェブサイトの脆弱性の届出に関して、IPA が通知を行い、ウェブサイト運営者が 2009 年第 4 四半期に修正を完了したものが 431 件（累計 2,654 件）でした。

2004 年 7 月の届出受付開始から 5 年半が経過し、修正完了件数の全累計が 3,054 件となりました。このうち、1,000 件は 2009 年に修正を完了しています。**修正完了件数が年々増加しており、制度として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)脆弱性関連情報の届出状況

2009 年第 4 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 24 件、ウェブアプリケーション（ウェブサイト）に関するもの 127 件、合計 151 件でした（表 1）。

**表 1. 2009 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 | **24** 件 | **1,018** 件 |
| ウェブサイト | **127** 件 | **4,959** 件 |
| 合計 | **151** 件 | **5,977** 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 1,018 件、ウェブサイトに関するもの 4,959 件、合計 5,977 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 1）。2008 年第 3 四半期から 2009 年第 2 四半期にかけて 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。1 就業日あたりの届出件数は 2009 年第 4 四半期末で 4.47 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 |
|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |

[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（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/

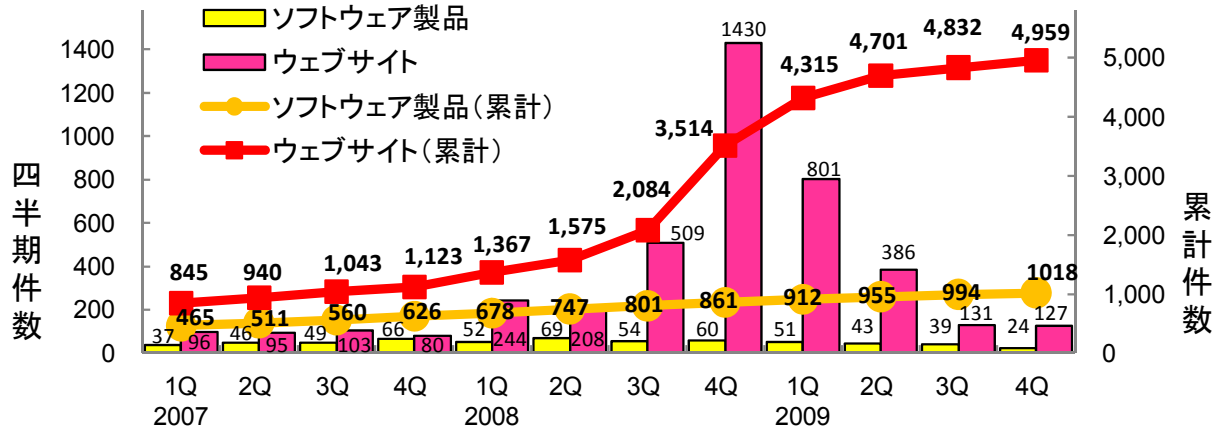



図1.脆弱性関連情報の届出件数の四半期別推移

**(3)個人情報を扱っているウェブサイト運営者は包括的な脆弱性対策および設定状況の再確認を**

2009 年の一年間に、ウェブサイトに関する脆弱性関連情報の届出が 1,445 件ありました。このうち SQL インジェクションの脆弱性に関する届出が 168 件あり、その中で、IPA が個人情報を取扱っていると判断した届出[3]は 103 件（61%）ありました（図 2）。

個人情報を取り扱っているにもかかわらず、発見された SQL インジェクションの脆弱性が放置されたままのウェブサイトが 41 件あります。そのウェブサイト運営主体ごとの割合は、企業が 25 件（61%）、団体（協会・社団法人）が 8 件（20%）、地方公共団体が 5 件（12%）などとなっています（図 3）。

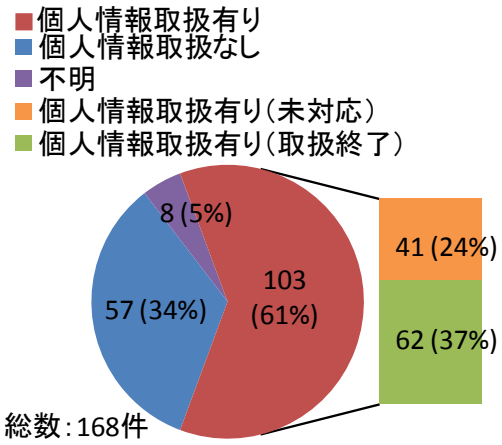



図2. 個人情報取扱の割合

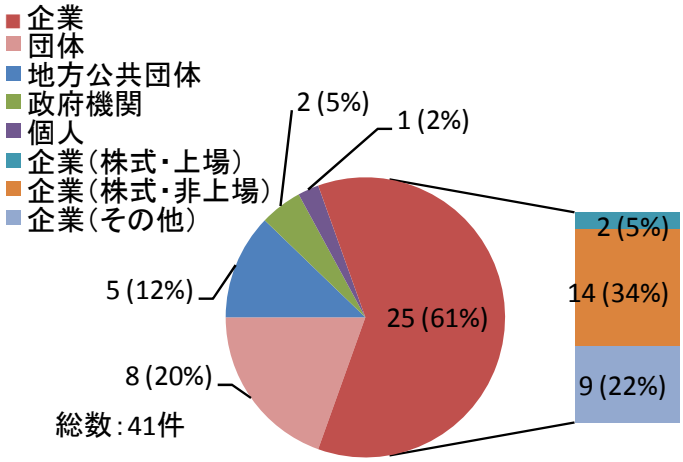



図3. SQLインジェクション未対応の割合

その他、2009 年の 1 年間に個人情報が漏えいしているという届出が 6 件ありました。個人情報が漏えいした脆弱性の内訳は、ファイルの誤った公開が 2 件、認証に関する不備が 2 件、セッション管理の不備が 1 件、アクセス制限の回避が 1 件でした。

**個人情報などの重要情報を取り扱っているウェブサイトは、個人情報保護法を遵守する観点からも、包括的なウェブサイトの脆弱性対策および設定状況の再確認が必要です。**

**(4)ソフトウェア製品開発者は認証・認可機能の再確認を**

2009 年の一年間に、ソフトウェア製品に関する脆弱性関連情報の届出が 161 件ありました。脆弱性の種類で分類すると、クロスサイト・スクリプティングが 72 件（45%）、認証・認可の不備に関するものが 15 件（9%）、ディレクトリ・トラバーサルが 12 件（7%）などとなっています（図 4）。このうち、

[3] IPA では、プライバシーポリシーの記載内容や、住所・氏名等を入力するフォームの有無から、個人情報の取扱有無を判断しました。

**認証・認可の不備は、重要な情報資産に対するアクセス制御を無効化するもので、特に注意が必要です。**

2009 年の一年間に、JVN で脆弱性対策情報を公開したものの中でも、認証・認可の不備に関するものが 11 件（14%）あり、第 2 位となっています（図 5）。

例えば、JVN で公表した「EC-CUBE」における情報漏えいの脆弱性[4]では、認証の欠落により第三者に顧客情報が閲覧されてしまう可能性がありました。また、「SEIL/B1」の認証処理における脆弱性[5]では、認証が適切に行われないために、第三者に認証が必要なネットワークにアクセスされる可能性がありました[6]。**製品開発者は、認証・認可の機能を正しく実装する必要があります。**

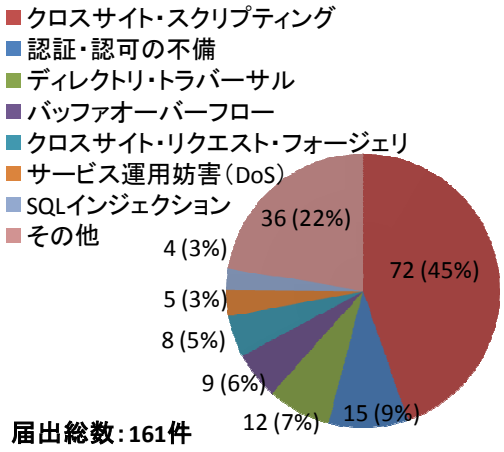



図4. ソフトウェア製品 届出 脆弱性別内訳

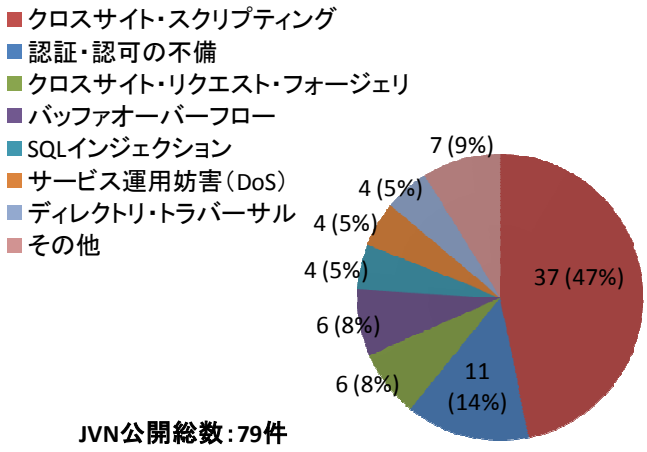



図5 .2009年 JVN公開 脆弱性別内訳

**(5)脆弱性対策情報の収集に JVN をグローバルに活用して頂くことが可能になりました（CVE 互換認定）**

共通脆弱性識別子 CVE[7]は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子です。1999 年の運用開始以来、10 年が経過しました。国内外の脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用しています。

この度、**JVN、JVN iPedia、MyJVN において、該当する CVE 識別番号が適切に関連付けられていることなどが MITRE 社より認定されました（CVE 互換認定）。**

http://www.cve.mitre.org/news/index.html#jan082010a

CVE 互換認定を受けたことにより、CVE を用いた脆弱性対策情報の検索や、脆弱性情報が同じ脆弱性に関するものであるか否かの判断などに、**JVN をグローバルに活用して頂くことが可能になりました。**

今後も CVE 等の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。

■ 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

[4] http://jvn.jp/jp/JVN79762947/index.html
[5] http://jvn.jp/jp/JVN49602378/index.html
[6] これらは製品開発者自身からの届出です。利用者に広く対策情報を公開するため JVN が活用されています。
[7] Common Vulnerabilities and Exposures。脆弱性情報を一意に特定するための標準仕様で、各脆弱性に対して CVE 識別番号を付与したリスト。概要は次を参照下さい。 http://www.ipa.go.jp/security/vuln/CVE.html

## 1.ソフトウェア製品の脆弱性の処理状況

2009 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が 16 件（累計 400 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 2 件（累計 37 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 3 件[8]（累計 151 件）でした。これらの取扱いを終了したものの合計は 21 件（累計 605 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 | 16 件 | 400 件 |
| | 個別対応 | 0 件 | 17 件 |
| 脆弱性ではない | | 2 件 | 37 件 |
| 不受理 | | 3 件 | 151 件 |
| 合計 | | 21 件 | 605 件 |

この他、海外の CSIRT[9]から JPCERT/CC が連絡を受けた 15 件（累計 456 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。

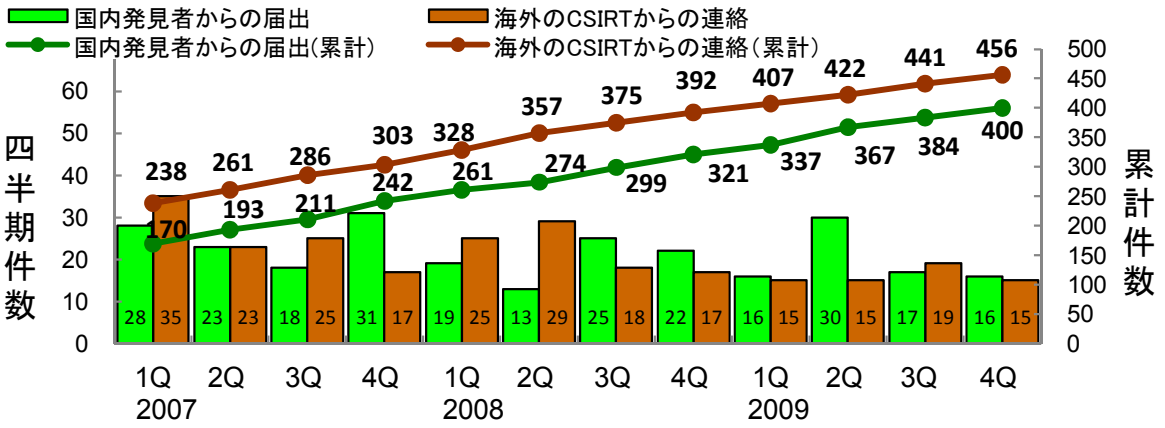



図6.ソフトウェア製品の脆弱性対策情報の公表件数

### 1.1 製品開発者自身の脆弱性対策情報の届出状況

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届出を行ったものに関して、今四半期は(1)SEIL/X シリーズおよび SEIL/B1 におけるバッファオーバーフローの脆弱性[10]、(2)SEIL/X シリーズおよび SEIL/B1 におけるサービス運用妨害（DoS）の脆弱性[11]、(3)SEIL/B1 の認証処理における脆弱性[12]、(4)EC-CUBE における情報漏えいの脆弱性[13]の 4 件（累計 32 件）の脆弱性対策情報を JVN で公表しました。

**今後も、利用者への周知のために製品開発者が JVN を活用されることを期待します。**

### 1.2 組込みソフトウェアの脆弱性対策情報の公表状況

組込みソフトウェアに関して、今四半期は 1.1 の(1)～(3)の 3 件の脆弱性対策情報の公表を行い、累計で 26 件となりました（図 7）。

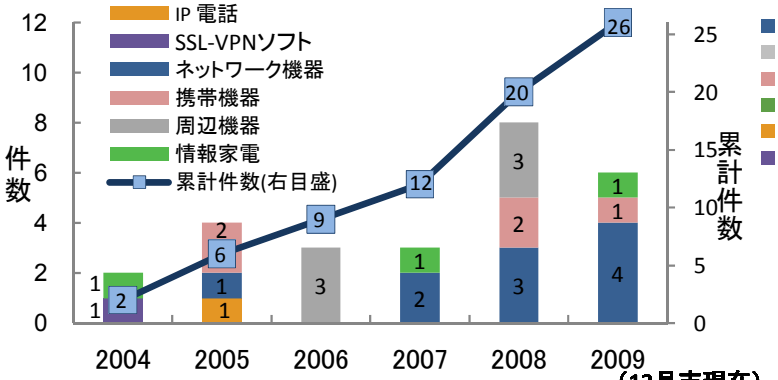
組込みソフトウェアの内訳は、図 8 に示すように、ルータやスイッチなどのネットワーク機器

---

[8] 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 1 件の合計です。
[9] 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。
[10] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=9.3、別紙 P.11 表 1-2 項番 1 を参照下さい。
[11] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.8、別紙 P.11 表 1-2 項番 2 を参照下さい。
[12] 本脆弱性の深刻度=レベル I（注意）、CVSS 基本値=2.6、別紙 P.13 表 1-2 項番 16 を参照下さい。
[13] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=5.0、別紙 P.12 表 1-2 項番 6 を参照下さい。

が 10 件、プリンタやハードディスクなどの周辺機器が 6 件、携帯電話や携帯端末などの携帯機器が 5 件、DVD レコーダやネットワークカメラなどの情報家電が 3 件などとなっています。

今後、インターネットに接続される情報家電が増えると、組込みソフトウェアの脆弱性を狙う攻撃の顕在化が予測されます。**組込み機器ではパッチの適用が困難なケースもあり、組込みソフトウェアの開発者は、製品の開発段階から脆弱性を作り込まないようなセキュリティの考慮が必要です。**




（12月末現在）

図7.組込みソフトウェアの脆弱性の修正完了件数

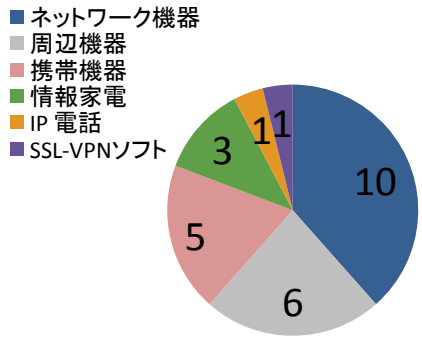



図8.組込みソフトウェアの脆弱性の対象機器

## 2.ウェブサイトの脆弱性の処理状況

2009 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が 431 件（累計 2,654 件）、IPA が注意喚起等を行った後に処理を終了したものが 791 件[14]（累計 1,119 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 26 件（累計 217 件）、ウェブサイト運営者と連絡が不可能なものが 5 件（累計 16 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 9 件[15]（累計 133 件）でした。

これらの取扱いを終了したものの合計は 1,262 件（累計 4,139 件）です（表 4）。これらのうち、修正完了件数の期別推移を図 9 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 | **431** 件 | **2,654** 件 |
| 注意喚起 | **791** 件 | **1,119** 件 |
| 脆弱性ではない | **26** 件 | **217** 件 |
| 連絡不可能 | **5** 件 | **16** 件 |
| 不受理 | **9** 件 | **133** 件 |
| 合計 | **1,262** 件 | **4,139** 件 |

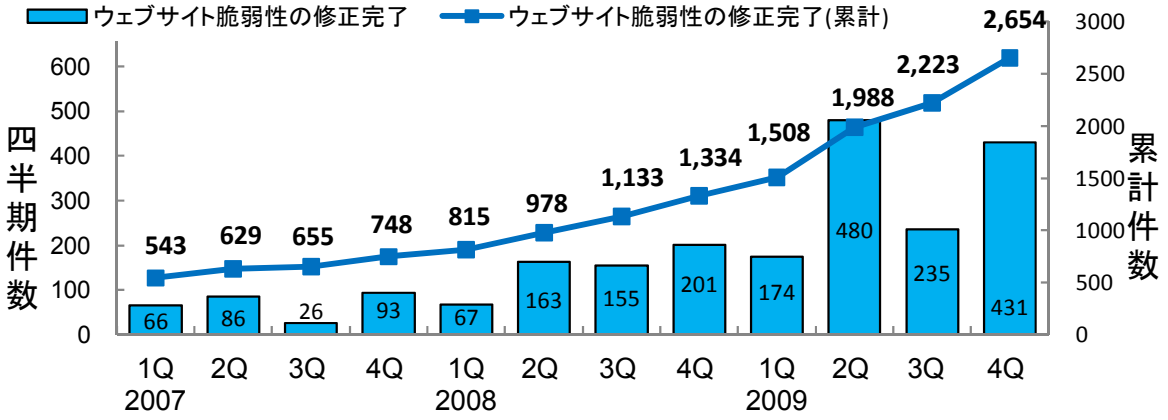



図9.ウェブサイトの脆弱性の修正完了件数

[14] ウェブサイトで利用されている DNS サーバの既知の脆弱性への注意喚起（http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.html）

[15] 今期の届出の中で不受理としたものは 8 件、前期までの届出の中で今期に不受理としたものは 1 件です。

## 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 IPA に届出のあったウェブサイトの脆弱性関連情報 127 件のうち、不受理のものを除いた 119 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 69 件（58%）、政府機関が 28 件（24%）、地方公共団体が 7 件（6%）、団体が 6 件（5%）などです（図 10）。

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 64 件（54%）、SQL インジェクションが 16 件（13%）、ファイルの誤った公開 11 件（9%）、認証に関する不備 6 件（5%）などです（図 11）。

**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。**

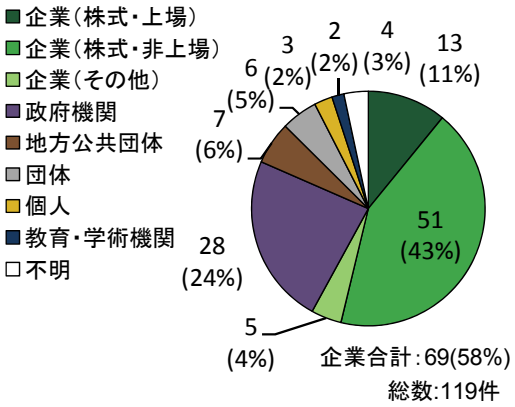



図10.ウェブサイトの運営主体（2009年4Q）

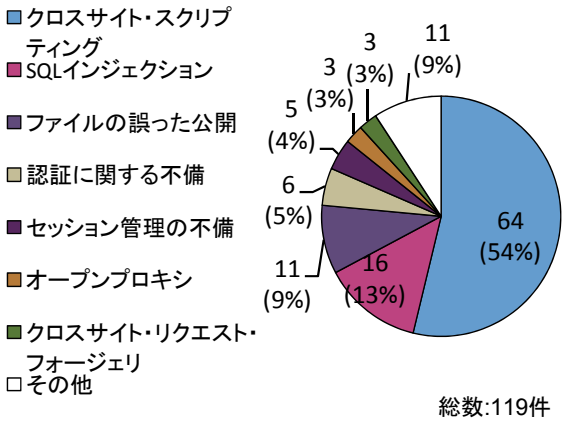



図11.ウェブサイトの脆弱性の種類（2009年4Q）

## 2.2 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 551 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丁寧に解説するなど、1～2 カ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 12 に示します。経過日数が 90 日から 199 日に達したものは 92 件、200 日から 299 日のものは 144 件など、これらの合計は 551 件（前四半期は 1,125 件）です。前四半期のものは 591 件減少し、今四半期で新たに 17 件が 90 日以上となったため 574 件減少しました。

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。**

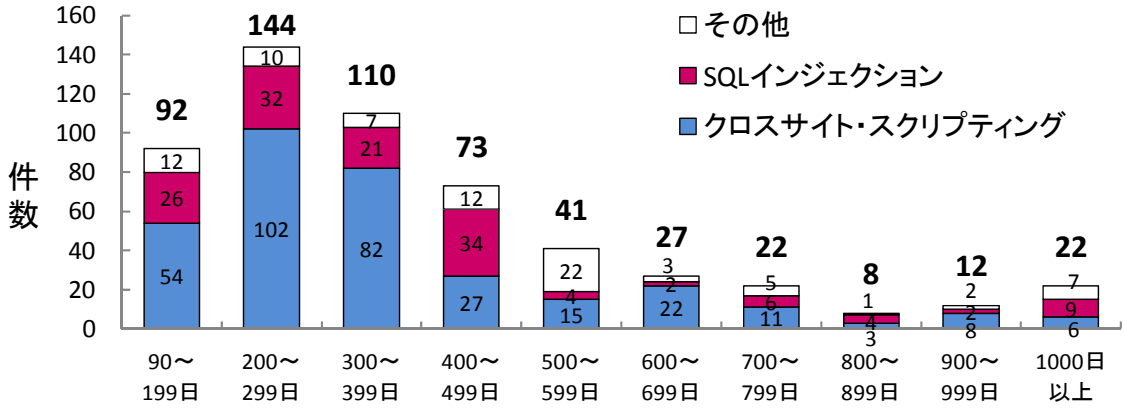



図12. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

なお、脆弱性関連情報の取扱いの効率化を図るため、2009 年 7 月 8 日の「情報セキュリティ早期警戒パートナーシップガイドラインの改訂[16]」で、このような一定期間にわたり的確な答えが無い場合は、その脆弱性の影響範囲や取扱期間を考慮し、1 年以上経過したものから順次取扱を終了します。

## 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、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および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[17]。

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[18]」で、IPA が公開している「脆弱性対策情報データベース JVN iPedia[19]」の 2009 年 4 月から 7 月までのアクセスログを解析した事例を示しましたが、図 13 に示すように 8 月以降も攻撃が継続しています。

2009 年の 1 年間では、2008 年頃から急増している SQL インジェクション攻撃[20]が 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[21]の情報を狙ったディレクトリ・トラバーサル攻撃が 38%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。

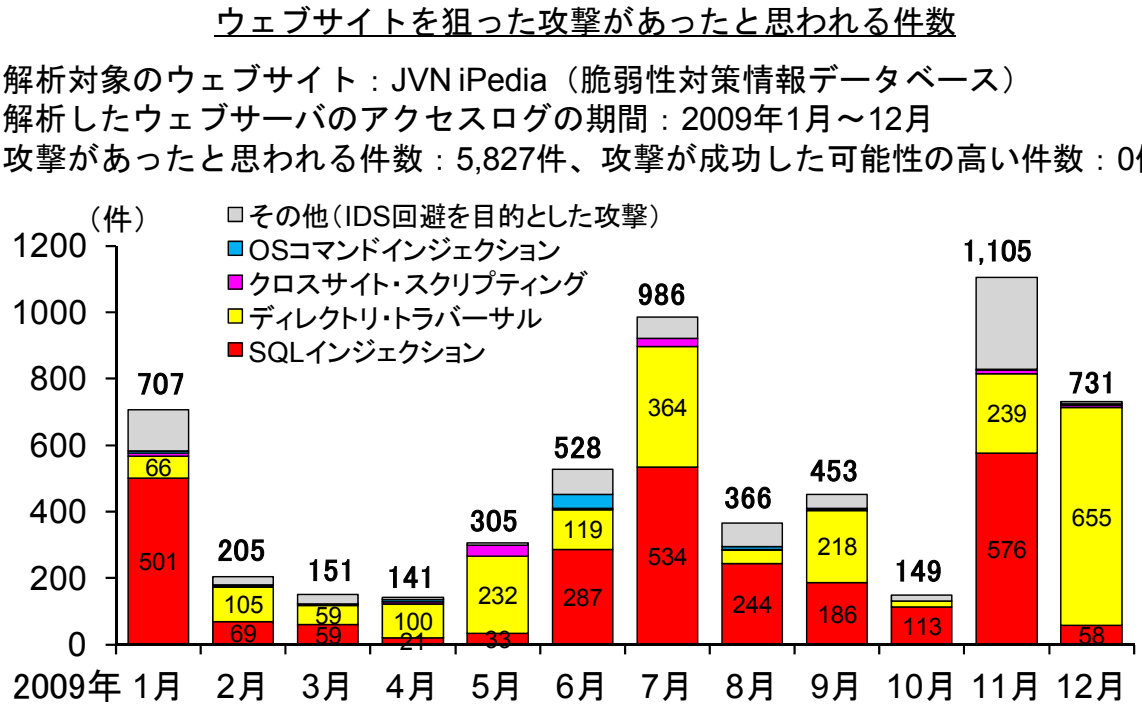



図13. SQLインジェクション検出ツール「iLogScanner」での解析事例

[16] 情報セキュリティ早期警戒パートナーシップガイドライン。
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

[17] 「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

[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

[19] 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/

[20] 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

[21] 具体的には、passwd ファイル、environ ファイル、resolv.con ファイルなど。

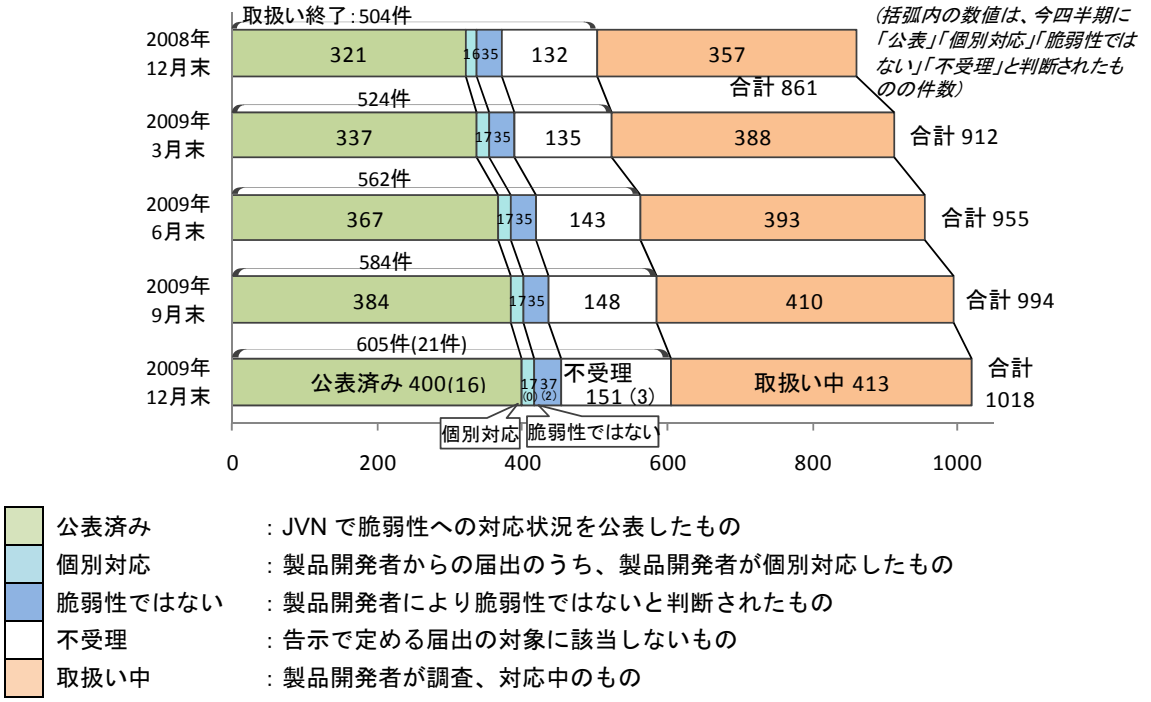
別紙 2

# 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 16 件（累計 400 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 2 件（累計 37 件）、「不受理」としたものは 3 件（累計 151 件）、取扱中は 413 件です。



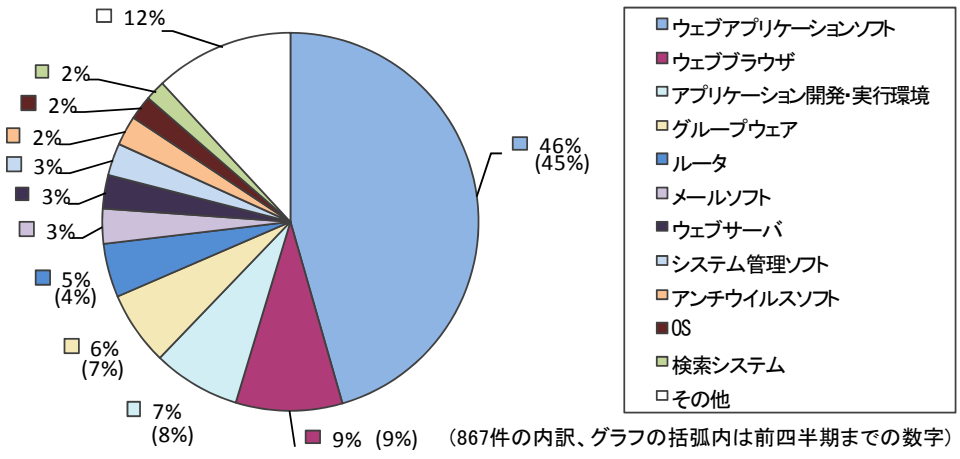

| | |
|---|---|
| 公表済み | ：JVN で脆弱性への対応状況を公表したもの |
| 個別対応 | ：製品開発者からの届出のうち、製品開発者が個別対応したもの |
| 脆弱性ではない | ：製品開発者により脆弱性ではないと判断されたもの |
| 不受理 | ：告示で定める届出の対象に該当しないもの |
| 取扱い中 | ：製品開発者が調査、対応中のもの |

**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 1,018 件のうち、不受理のものを除いた 867 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。




（867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12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 1,018 件のうち、不受理のものを除いた 867 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 10 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。

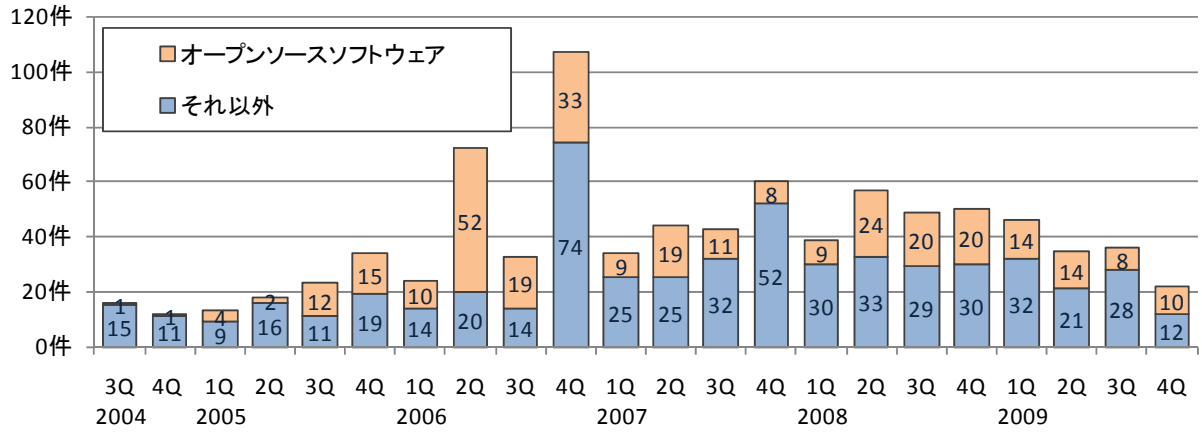
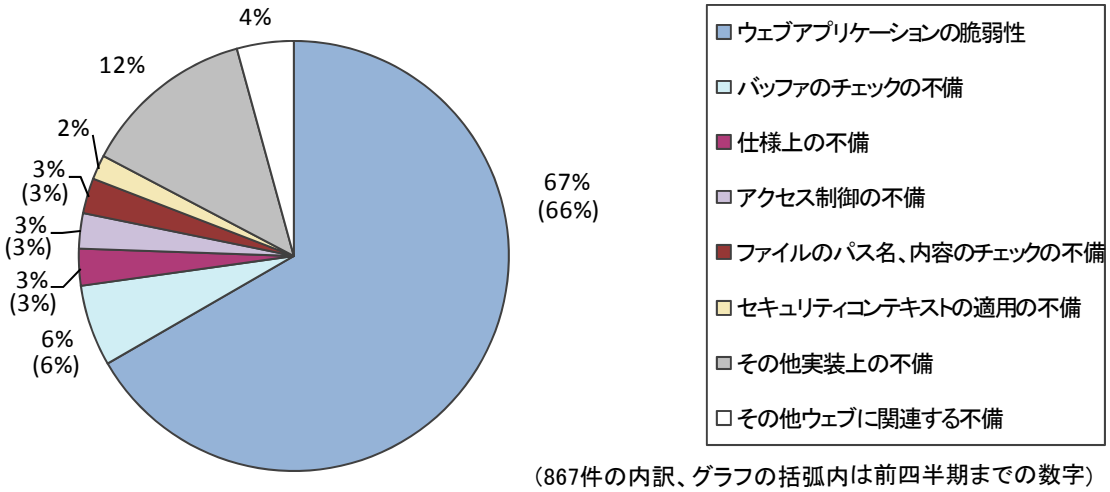



**図1-3.オープンソースソフトウェアの脆弱性の届出件数**　（867件の内訳）

## 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 1,018 件のうち、不受理のものを除いた 867 件の原因別[22]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」が最も多いです。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。




（867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12月末まで）**

[22] 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。

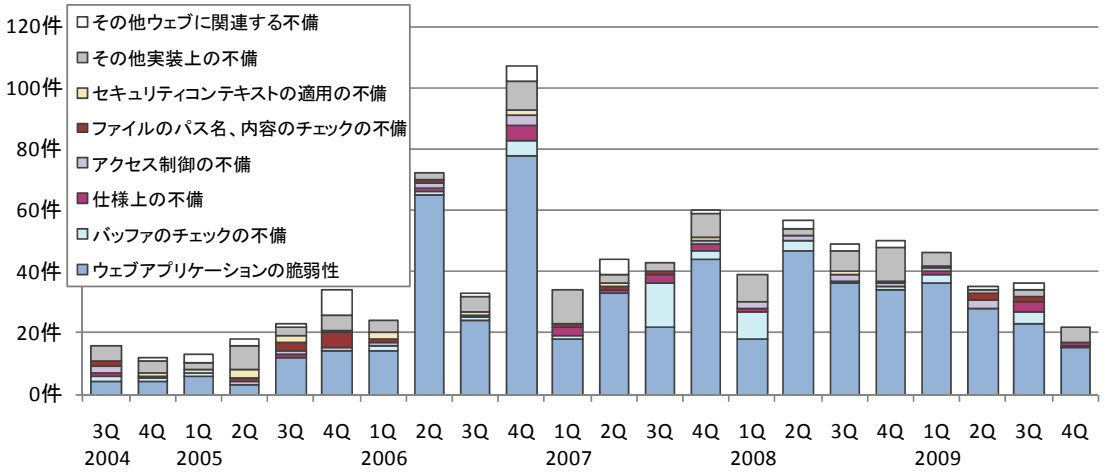
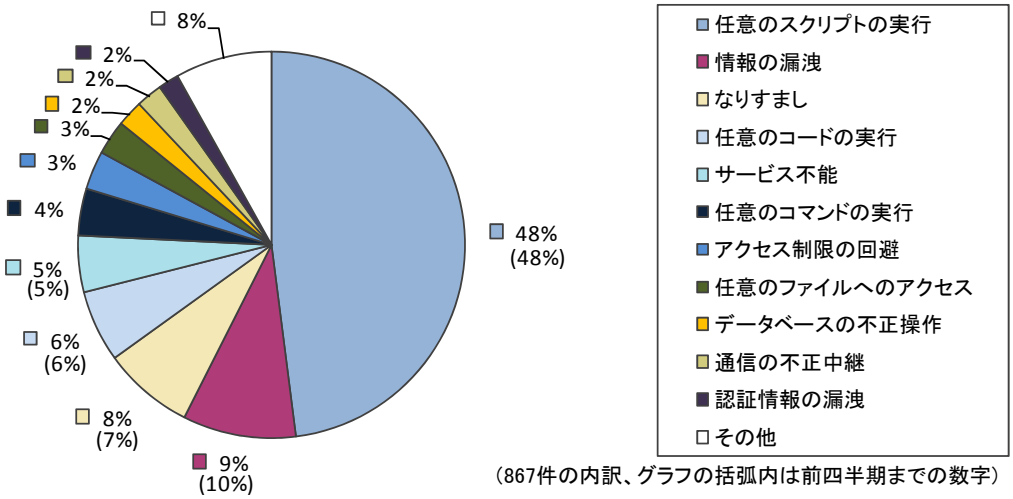



**図1-5. ソフトウェア製品の脆弱性 原因別届出件数の推移（届出受付開始から2009年12月末まで）**




（867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 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 | 16 件 | 400 件 |
| ② | 海外 CSIRT 等と連携して公表したもの | 15 件 | 456 件 |
| | 合計 | 31 件 | 856 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 |
|---|---|---|---|---|---|
| 32% | 32% | 33% | 34% | 35% | 35% |

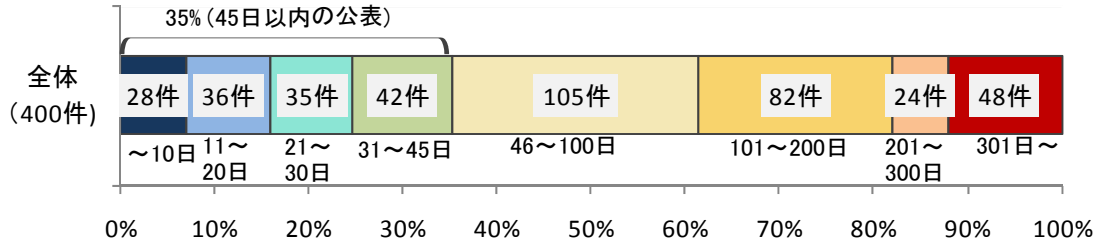



**図1-7. ソフトウェア製品の脆弱性公表日数**

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 6 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）、複数開発者・製品に影響がある脆弱性が 1 件（表 1-2 の*3）、組込みソフトウェア製品の脆弱性が 3 件（表 1-2 の*4）ありました。

**表 1-2.2009 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 (*2) (*4) | 「SEIL/X シリーズ」および「SEIL/B1」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/X シリーズ」および「SEIL/B1」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、当該製品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 10 月 28 日 | 9.3 |
| 2 (*2) (*4) | 「SEIL/X シリーズ」および「SEIL/B1」におけるサービス運用妨害 (DoS) の脆弱性 | ルータ製品「SEIL/X シリーズ」および「SEIL/B1」には、サービス運用妨害 (DoS) の脆弱性がありました。このため、遠隔の第三者により細工されたパケットを送られることで、サービス不能状態になる可能性がありました。 | 2009 年 10 月 28 日 | 7.8 |
| 脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9 | | | | |
| 3 | キヤノン IT ソリューションズ製「ACCESSGUARDIAN」におけるクロスサイト・スクリプティングの脆弱性 | ウェブセキュリティゲートウェイ製品「ACCESSGUARDIAN」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 10 月 20 日 | 4.3 |
| 4 (*3) | IPv6 を実装した複数の製品にサービス運用妨害 (DoS) の脆弱性 | IPv6 を実装した複数の製品には、サービス運用妨害 (DoS) の脆弱性がありました。このため、第三者により大量のパケットを送られることで、サービス不能状態になる可能性がありました。 | 2009 年 10 月 26 日 | 5.7 |
| 5 (*1) | 「Redmine」におけるクロスサイト・スクリプティングの脆弱性 | プロジェクト管理ソフト「Redmine」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 11 月 19 日 | 4.0 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 6 (*1) (*2) | 「EC-CUBE」における情報漏えいの脆弱性 | ショッピングサイト構築ソフト「EC-CUBE」には、情報漏えい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に保存されている顧客情報が漏えいする可能性がありました。 | 2009 年 12 月 7 日 | 5.0 |
| 7 | 「Active! mail 2003」におけるクロスサイト・スクリプティングの脆弱性 | ウェブメールソフト「Active! mail 2003」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 12 月 8 日 | 4.3 |
| 8 | 「Active! mail 2003」におけるセッション ID 漏えいの脆弱性 | ウェブメールソフト「Active! mail 2003」には、セッション ID 漏えい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のユーザになりすまされる可能性がありました。 | 2009 年 12 月 8 日 | 4.0 |
| 9 | 「Active! mail 2003」における Cookie 漏えいの脆弱性 | ウェブメールソフト「Active! mail 2003」には、Cookie 漏えい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のユーザになりすまされる可能性がありました。 | 2009 年 12 月 8 日 | 4.0 |
| 10 | 「P forum」におけるディレクトリ・トラバーサルの脆弱性 | 電子掲示板ソフト「P forum」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。 | 2009 年 12 月 15 日 | 5.0 |
| 脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9 | | | | |
| 11 (*1) | 「SugarCRM」におけるクロスサイト・スクリプティングの脆弱性 | 顧客管理システム「SugarCRM」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 10 月 2 日 | 2.6 |
| 12 | 複数のサイボウズ製品におけるクロスサイト・スクリプティングの脆弱性 | 複数のサイボウズ製品には、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 10 月 15 日 | 2.6 |
| 13 (*1) | 「Roundcube Webmail」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 | ウェブメールソフト「Roundcube Webmail」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。項番 14 で修正された問題とは異なります。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、意図せず情報が登録される可能性がありました。 | 2009 年 11 月 4 日 | 2.6 |
| 14 (*1) | 「Roundcube Webmail」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 | ウェブメールソフト「Roundcube Webmail」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。項番 13 で修正された問題とは異なります。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、意図せずメールが送信される可能性がありました。 | 2009 年 11 月 4 日 | 2.6 |
| 15 (*1) | 「Redmine」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 | プロジェクト管理ソフト「Redmine」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、意図せず任意のチケットを削除される可能性がありました。 | 2009 年 11 月 19 日 | 2.6 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 16 (*2) (*4) | 「SEIL/B1」の認証処理における脆弱性 | ルータ製品「SEIL/X シリーズ」および「SEIL/B1」には、機能の実装上の問題により認証が適切に行われない脆弱性がありました。このため、第三者により認証が必要なネットワークにアクセスされる可能性がありました。 | 2009 年 12 月 9 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）：複数開発者・製品に影響がある脆弱性
（*4）：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 15 件には、通常の脆弱性情報 9 件（表 1-3）と、対応に緊急を要する Technical Cyber Security Alert（表 1-4）の 6 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[23]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 | Wireshark の erf ファイル処理に脆弱性 | 注意喚起として掲載 |
| 2 | Adobe Reader および Acrobat の複数の JavaScript メソッドに脆弱性 | 注意喚起として掲載 |
| 3 | SSL および TLS プロトコルに脆弱性 | 複数製品開発者へ通知 |
| 4 | Microsoft Internet Explorer に脆弱性 | 緊急案件として掲載 |
| 5 | 複数の SSL VPN (Web VPN) 製品においてウェブブラウザのセキュリティが迂回される問題 | 複数製品開発者へ通知 |
| 6 | BIND 9 の DNSSEC 検証処理における脆弱性 | 複数製品開発者へ通知 |
| 7 | NTP 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 |
| 8 | Indeo コーデックに複数の脆弱性 | 注意喚起として掲載 |
| 9 | Adobe Reader および Acrobat 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 |

**表 1-4.米国 US-CERT[24]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 | 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 |
| 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 | Oracle 製品における複数の脆弱性に対するアップデート |
| 4 | Microsoft 製品における複数の脆弱性に対するアップデート |
| 5 | Microsoft 製品における複数の脆弱性に対するアップデート |
| 6 | Adobe Flash に複数の脆弱性 |

[23] 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。
[24] 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

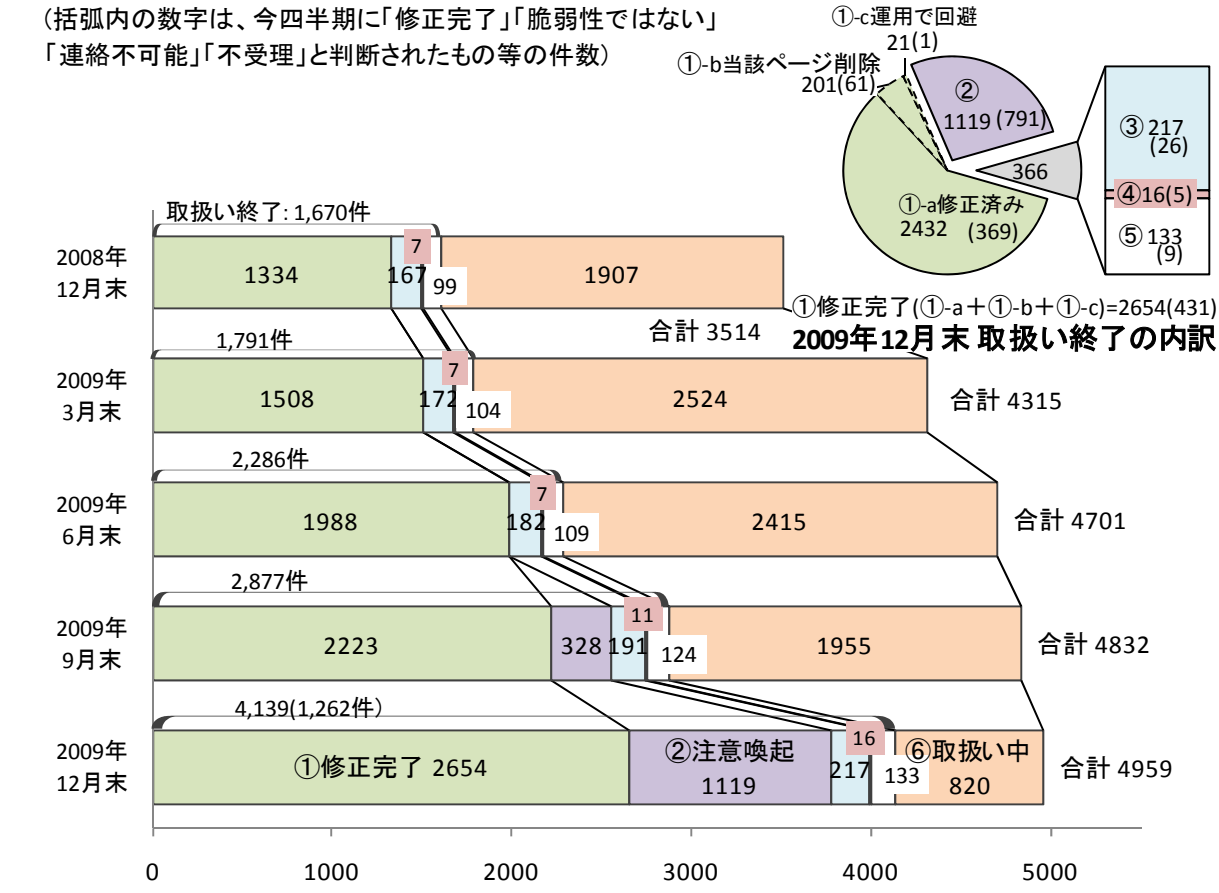
### 2.1 ウェブサイトの脆弱性の処理状況

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 1,262 件（累計 4,139 件）でした。このうち、「修正完了」したものは 431 件（累計 2,654 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 791 件（累計 1,119 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 26 件（累計 217 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 5 件（累計 16 件）です。「不受理」としたものは 9 件（累計 133 件）でした。

取扱いを終了した累計 4,139 件のうち、「注意喚起」「連絡不可能」「不受理」を除く累計 2,871 件（69%）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 61 件（累計 201 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 21 件）でした。

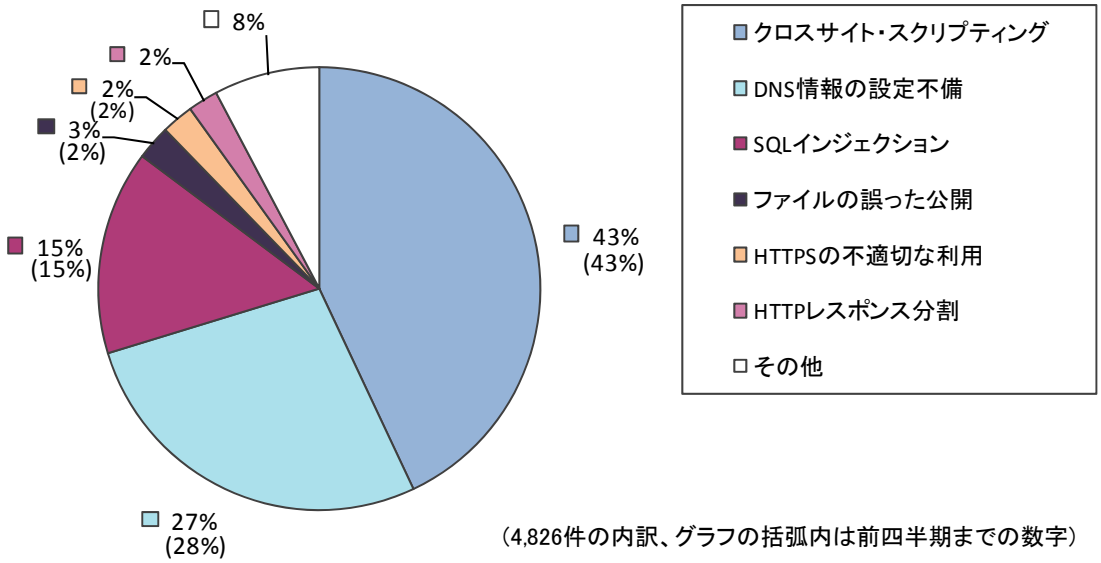



| | | |
|---|---|---|
| ①修正完了 | ： | ウェブサイト運営者により脆弱性が修正されたもの |
| -a 修正済み | ： | 修正完了のうち、修正されたと判断したもの |
| -b 該当ページを削除 | ： | 修正完了のうち、当該ページを削除して対応したもの |
| -c 運用で回避 | ： | 修正完了のうち、運用により被害を回避しているもの |
| ②注意喚起 | ： | IPA による注意喚起で広く対策を促した後、処理を取りやめたもの |
| ③脆弱性ではない | ： | IPA およびウェブサイト運営者が脆弱性はないと判断したもの |
| ④連絡不可能 | ： | 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**

## 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 4,959 件のうち、不受理のものを除いた 4,826 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[25]。




（4,826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12月末まで）**

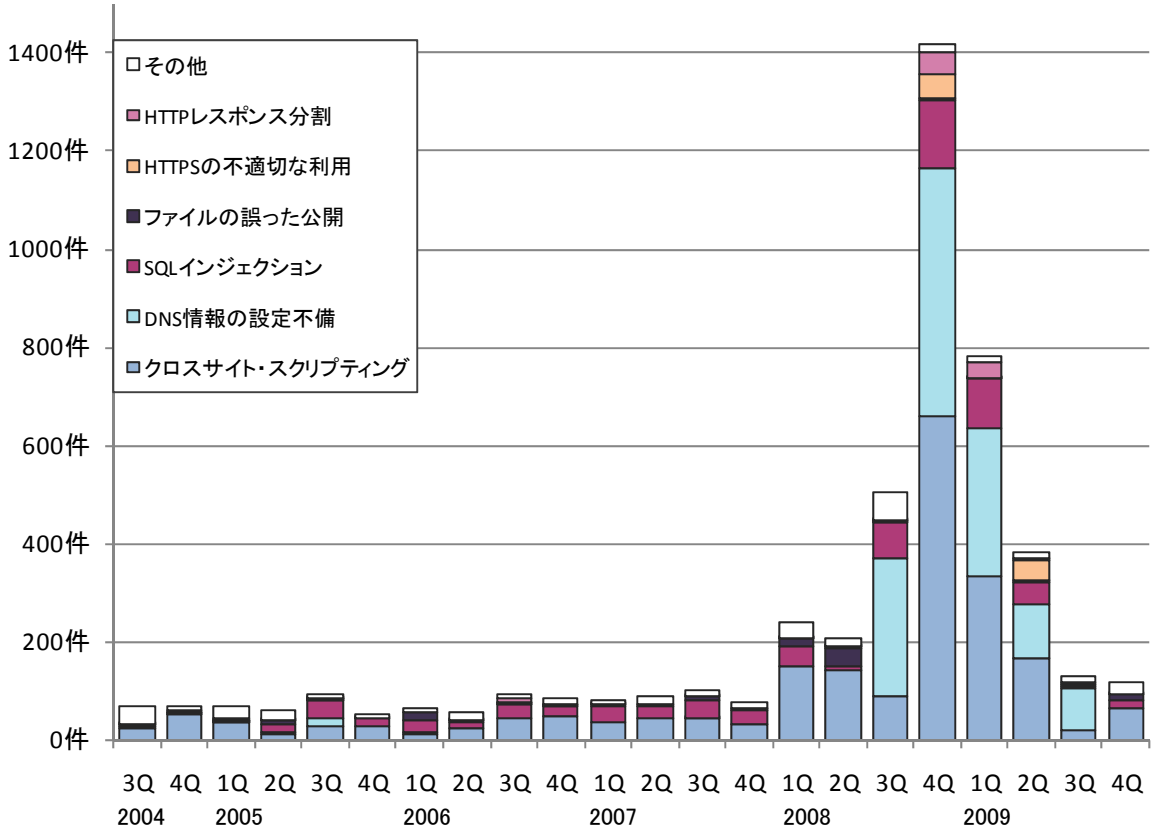
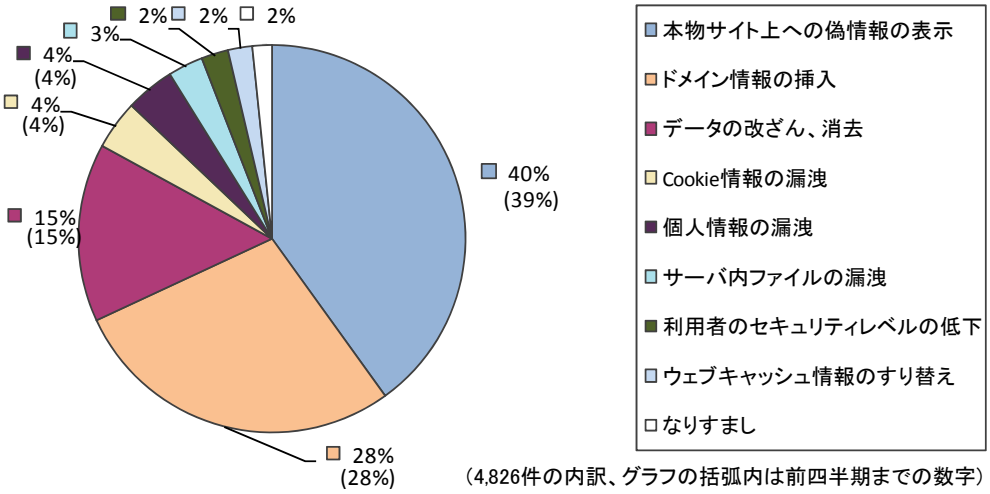



**図2-3.ウェブサイトの脆弱性 種類別届出件数の推移（届出受付開始から2009年12月末まで）**

[25] 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。




（4,826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2009年12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 87%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 2,654 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[26]。全体の 51%の届出が 30 日以内、全体の 72%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 |
|---|---|---|---|---|---|---|---|
| 77% | 81% | 80% | 83% | 80% | 79% | 79% | 72% |

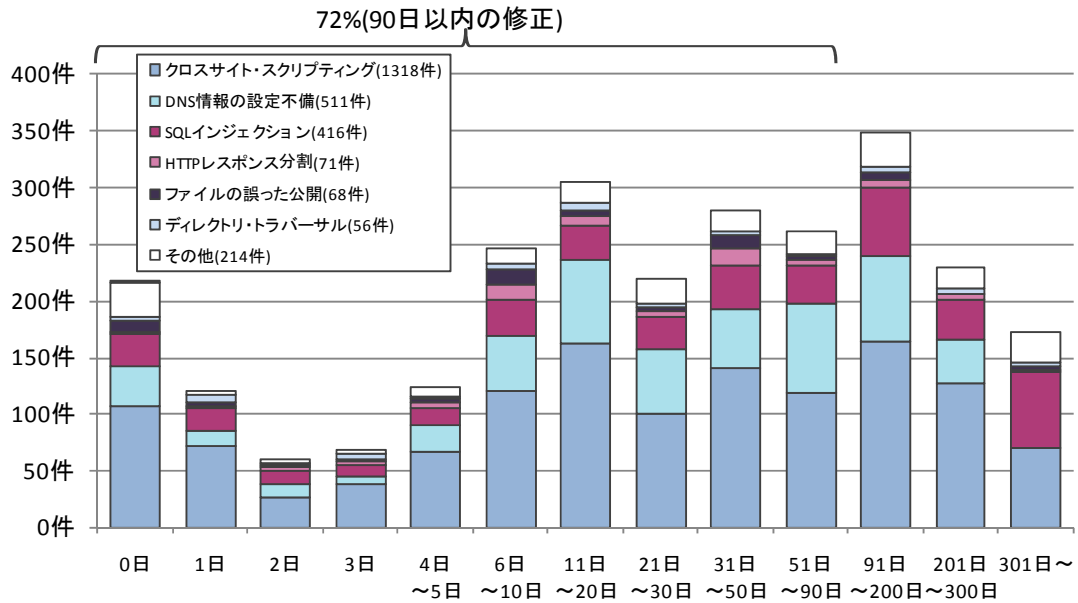



**図2-5.ウェブサイトの修正に要した日数**

[26] 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。

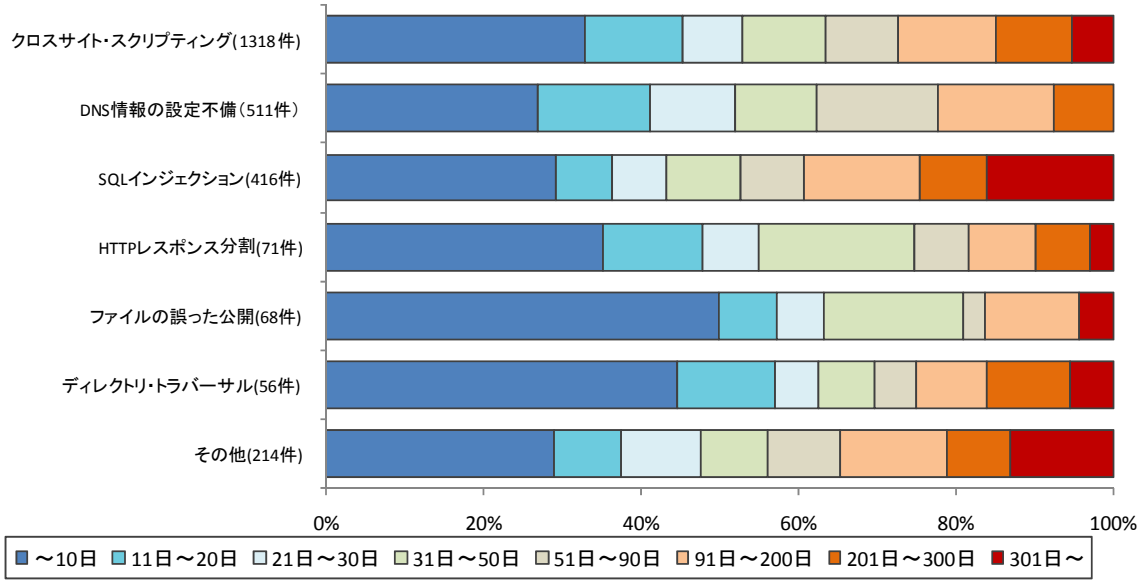



**図2-6.ウェブサイトの修正に要した脆弱性種類別の日数の傾向**

## 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/

### （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<br>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<br>通信の不正中継<br>なりすまし<br>任意のスクリプトの実行<br>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<br>価格等の改ざん<br>サービス不能<br>資源の枯渇<br>重要情報の漏洩<br>情報の漏洩<br>セッション・ハイジャック<br>通信の不正中継<br>なりすまし<br>任意のコマンドの実行<br>任意のスクリプトの実行<br>任意のファイルへのアクセス<br>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<br>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<br>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<br>情報の漏洩<br>任意のコードの実行<br>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<br>任意のコードの実行<br>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<br>サービス不能<br>資源の枯渇<br>任意のファイルへのアクセス<br>認証情報の漏洩 |

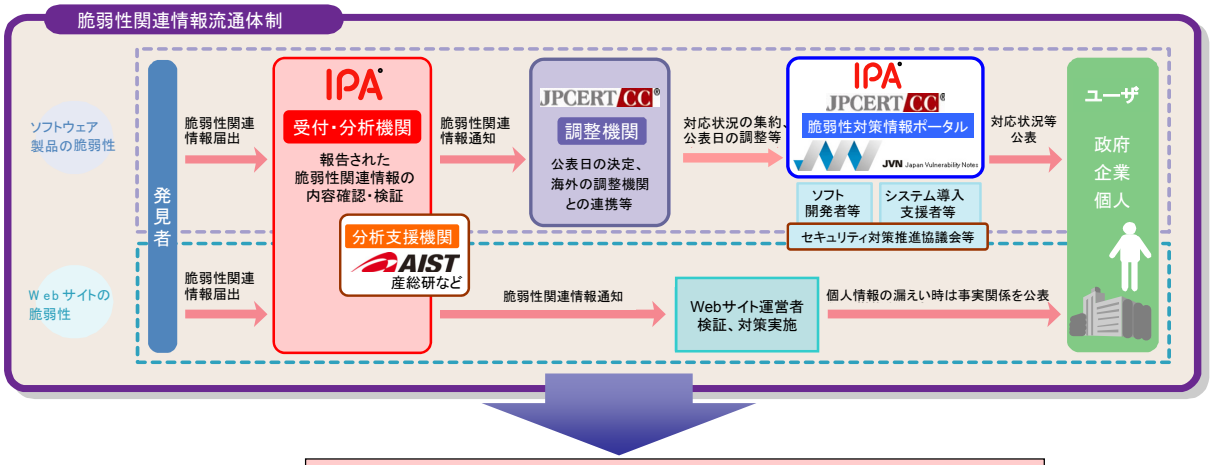
**付表 2 ウェブサイト脆弱性の分類**

| | 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<br>サーバ内ファイルの漏洩<br>データの改ざん、消去<br>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<br>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<br>個人情報の漏洩<br>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<br>サーバ内ファイルの漏洩<br>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<br>サーバ内ファイルの漏洩<br>個人情報の漏洩<br>データの改ざん、消去<br>なりすまし<br>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<br>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<br>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