プレスリリース
2009 年 4 月 21 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 [2009 年第 1 四半期(1 月～3 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、2009 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。

今四半期（2009 年 1 月 1 日から 3 月 31 日まで）に届出を受理したウェブサイトの脆弱性は 821 件でした。これらの脆弱性の種類は、DNS[2]の設定不備（DNS キャッシュポイズニングの脆弱性）が 343 件（42%）、クロスサイト・スクリプティングが 334 件（41%）、SQL インジェクションが 100 件（12%）となっており、この 3 種類の脆弱性の合計で 95%を占めています（別紙：図 7）。

ウェブサイト運営者や DNS サーバの管理者、ウェブアプリケーションの開発者は、これらの脆弱性対策の促進が、特に必要です。

(1)DNS の設定不備の届出が継続（別紙：図 10）

2008 年 7 月に複数の DNS サーバ製品の開発ベンダーから対策情報が公開された、DNS キャッシュポイズニングの脆弱性に関するものです。この対策情報の公開後、「実際に運用されている DNS サーバが、この脆弱性対策を実施していないのでは？」という旨の届出が継続しています。

ウェブサイト運営者や DNS サーバの管理者は、「DNS キャッシュポイズニング対策[3]」の資料を参考に、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。

(2)クロスサイト・スクリプティング脆弱性の届出が継続（別紙：図 11）

2000 年頃に報告された古典的な脆弱性で、多様な攻撃手法が知られており、近年も届出が継続しています。ウェブページの軽微な「出力処理」の追加で脆弱性を作り込んでしまった事例や、脆弱性対策が誤っていた事例などがありました。

ウェブアプリケーションの開発者は、「安全なウェブサイトの作り方[4]」の資料を参考に、クロスサイト・スクリプティング脆弱性への正しい対策が必要です。

(3)SQL インジェクション脆弱性の届出が継続（別紙：図 12）

この脆弱性を悪用した攻撃により、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いるものです。この被害報道と共に、「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？」という旨の届出が継続しています。

---

[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] Domain Name System。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] 「DNS キャッシュポイズニング対策」: http://www.ipa.go.jp/security/vuln/DNS_security.html
[4] 「安全なウェブサイトの作り方」: http://www.ipa.go.jp/security/vuln/websecurity.html

ウェブサイト運営者は、ウェブサーバのアクセスログ調査[5]およびウェブサイトの脆弱性検査等を行い、脆弱性が存在する場合は、SQL インジェクション対策の早急な実施が必要です。

(4)届出受付開始からの累計が 5,200 件に達しました

2009 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 51 件、ウェブアプリケーション（ウェブサイト）に関するもの 825 件、合計 876 件でした。

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 912 件、ウェブサイトに関するもの 4,339 件、合計 5,251 件となりました。ウェブサイトに関する届出が全体の 83%を占めています（表 1）。

表 1. 2009 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	**51** 件	**912** 件
ウェブサイト	**825** 件	**4,339** 件
計	**876** 件	**5,251** 件

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 2008 年 1Q までの**約 4 年間で 2,045 件でしたが、2008 年度（2008 年 2Q～2009 年 1Q）に 3,206 件の届出があり、累計で 5,251 件に達しました。**また、1 就業日あたりの届出件数は今四半期末で 4.55 件となりました（図 1）。

これは、2008 年 3Q 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、また、2008 年 4Q に一時的にクロスサイト・スクリプティングの脆弱性の届出が激増したためです。

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）

	2006/1Q	2007/1Q	2Q	3Q	4Q	2008/1Q	2Q	3Q	4Q	2009/1Q
累計届出件数[件]	685	1,310	1,451	1,603	1,749	2,045	2,322	2,885	4,375	5,251
1就業日あたり[件/日]	1.61	1.95	1.98	2.03	2.05	2.24	2.38	2.79	4.00	4.55

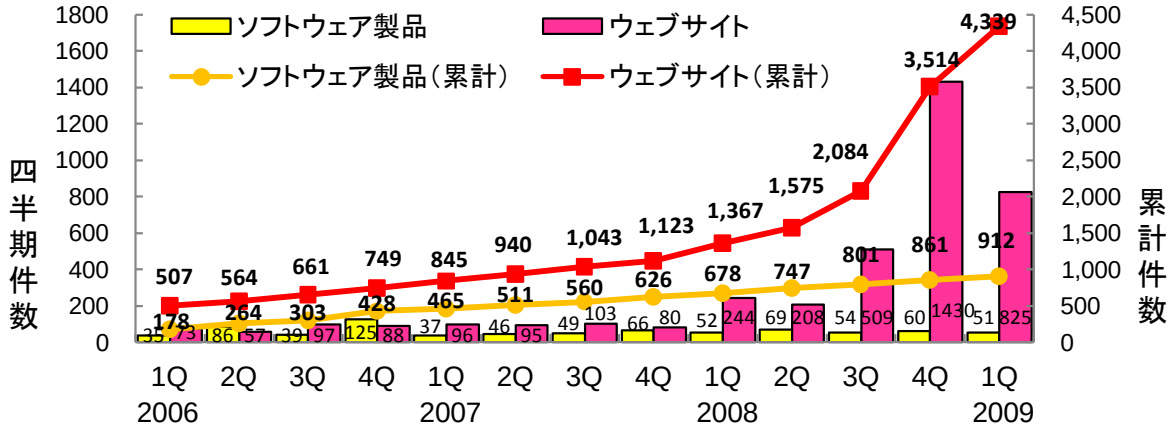


図1.脆弱性関連情報の届出件数の四半期別推移

■ 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 経営企画室 広報 江田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: pr@jpcert.or.jp

[5]「SQL インジェクション検出ツール iLogScanner」: http://www.ipa.go.jp/security/vuln/iLogScanner/

別紙

別紙１：届出のあった脆弱性の処理状況の概況

1.ソフトウェア製品の脆弱性の処理状況

2009 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 16 件（累計 337 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 1 件、製品開発者が脆弱性ではないと判断したものは 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 3 件でした。これらの取扱いを終了したものの合計は 20 件（累計 524 件）です（表 2）。

この他、海外の CSIRT[6]から JPCERT/CC が連絡を受けた **15** 件（累計 **407** 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 2 に示します。

表 2. 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	**337** 件
	個別対応	**1** 件	**17** 件
脆弱性ではない		**0** 件	**35** 件
不受理		**3** 件	**135** 件
合計		**20** 件	**524** 件

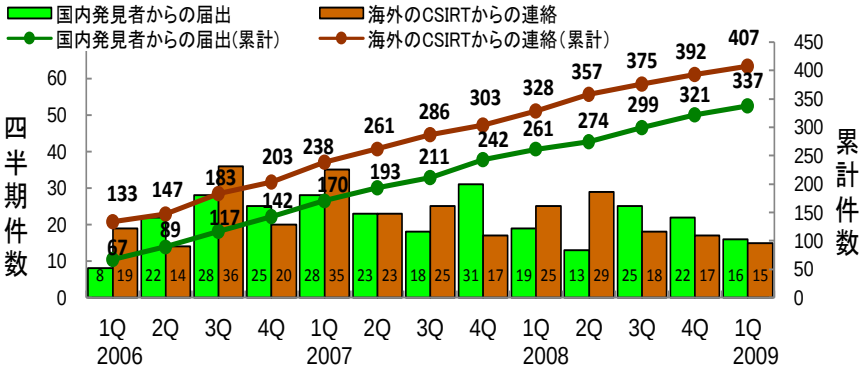


図2.ソフトウェア製品の脆弱性対策情報の公表件数

1.1 今四半期に JVN で対策情報を公表した主な脆弱性

(1) 複数の futomi's CGI Cafe 製のソフトウェアにおける管理者権限奪取の脆弱性[7]

ウェブサイト用検索ソフトやメールフォームソフトなど、複数の futomi's CGI Cafe 製のソフトウェアに、管理者権限が奪取可能である脆弱性が存在しました。この脆弱性が悪用されると、第三者によりそれぞれのソフトウェアの管理者になりすまされる可能性があり、1 月 23 日、3 月 10 日、3 月 31 日に JVN で対策情報を公表しました。

(2)「Becky! Internet Mail」におけるバッファオーバーフローの脆弱性[8]

有限会社リムアーツが提供する、メールを送受信するためのソフトウェア Becky! Internet Mail の機能に、バッファオーバーフローの脆弱性が存在しました。この脆弱性が悪用されると、メール送信者がメール受信者に対してメールの開封確認要求を行い、メール受信者が開封確認要求に応答した際に任意のコードが実行されてしまう可能性があり、2 月 12 日に JVN で対策情報を公表しました。

(3) ソニー製ネットワークカメラ SNC シリーズの 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[9]

ソニー株式会社が提供する、ネットワークカメラ SNC シリーズの ActiveX コントロールに、ヒープバッファオーバーフローの脆弱性が存在しました。この脆弱性が悪用されると、ウェブブラウザから ActiveX コントロールを利用したコンピュータ上で、任意のコードが実行されてしまう可能性があり、2 月 23 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。**

---

[6] 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。

[7] 本脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.5、別紙 P.8 表 1-2 項番 1、2、3 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 8 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=6.8、別紙 P.9 表 1-2 項番 9 を参照下さい。

1.2 組込みソフトウェアの脆弱性対策情報の公表状況

図 3 に示すように、今四半期は「Cisco IOS におけるクロスサイト・スクリプティングの脆弱性[10]」と「ソニー製ネットワークカメラ SNC シリーズの 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」の 2 件の脆弱性対策情報の公表を行い、累計で 23 件となりました。

組込みソフトウェアの内訳は、図 4 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が 9 件、プリンタやハードディスクなどの周辺機器が 5 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 4 件となっています。

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セキュリティの考慮が必要です。

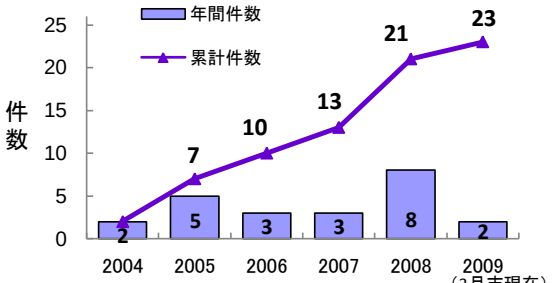


図3.組込みソフトウェアの脆弱性の修正完了件数

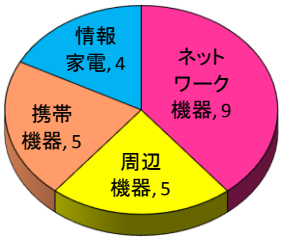


図4.組込みソフトウェアの脆弱性の対象機器

2.ウェブサイトの脆弱性の処理状況

2.1 届出の処理状況

2009 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は 174 件（累計 1,508 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 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 5 件[11]でした。

これらの取扱いを終了したものの合計は 184 件（累計 1,791 件）です（表 3）。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。

表3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	**174** 件	**1508** 件
脆弱性ではない	**5** 件	**172** 件
連絡不可能	**0** 件	**7** 件
不受理	**5** 件	**104** 件
合計	**184** 件	**1,791** 件

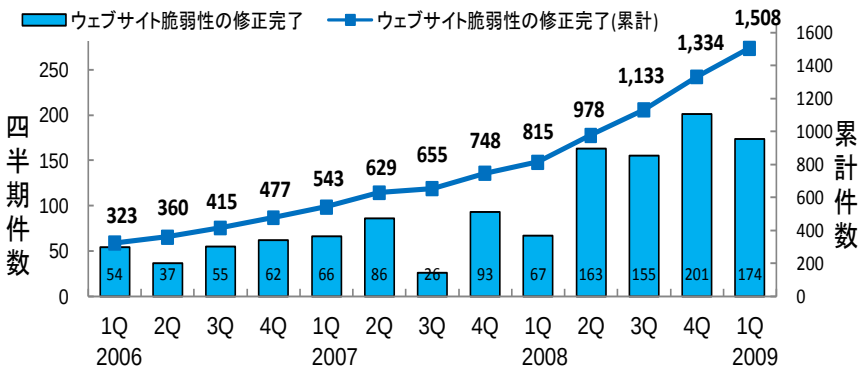


図5.ウェブサイトの脆弱性の修正完了件数

2.2 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対象ウェブサイト[12]の運営主体別内訳は、企業合計が 344 件（42%）、地方公共団体が 277 件（34%）、団体（協会・社団法人）が 79 件（10%）、教育・学術機関が 48 件（6%）、政府機関が 36 件（4%）などとなっています（　図 6）。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 343 件（42%）、クロスサイト・スクリプティングが 334 件（41%）、SQL インジェクションが 100 件（12%）などとなっています（図 7）。

ウェブサイト開発者は、広く知れ渡っている脆弱性を作り込まないような技術スキルを身につけたう

[10] 本脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.3、別紙 P.9 表 1-2 項番 7 を参照下さい。
[11] 今期の届出の中で不受理とした 4 件、先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。
[12] 今四半期に届出のあった 825 件の中の不受理 4 件を除いた 821 件の内訳です。

えで、ウェブサイトの企画・設計にあたることが必要です。

なお、クロスサイト・スクリプティング 334 件のうち 25 件は、2004 年 12 月に脆弱性対策情報が公表された「Namazu におけるクロスサイト・スクリプティングの脆弱性」のパッチ未適用のウェブサイトに対する届出です[13]。**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の脆弱性対策情報を収集し、未対策の場合はパッチの迅速な適用が必要です。**

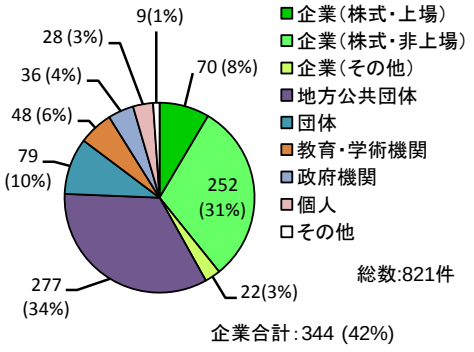


図6.ウェブサイトの運営主体(2009年第1四半期)

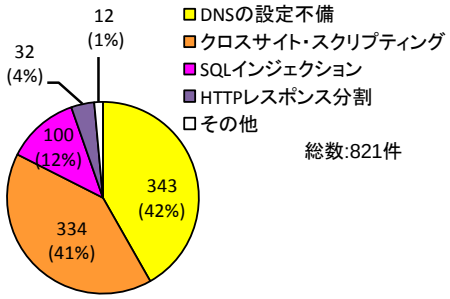


図7.ウェブサイトの脆弱性の種類(2009年第1四半期)

2.3 届出のあった対象ウェブサイトの運営者の半数が重要インフラ事業者等

今四半期に脆弱性の届出を受理した対象ウェブサイトを、重要インフラ（情報通信、金融、電力、航空など）の業種で分類すると、政府・行政サービスが 294 件、情報通信が 88 件、医療が 27 件、金融が 12 件などとなっており、届出の約半数を占めています（図 8）。なお、それらの脆弱性の種類の割合（図 9）は、全体での割合（図 7）とあまり変わりがありません。

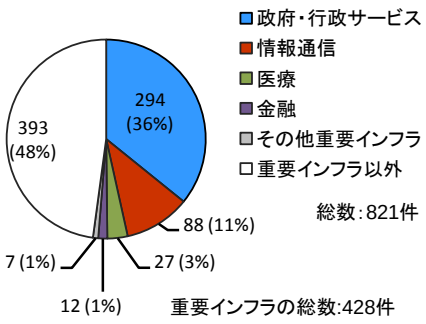


図8.ウェブサイトの重要インフラの業種での分類
(2009年第1四半期)

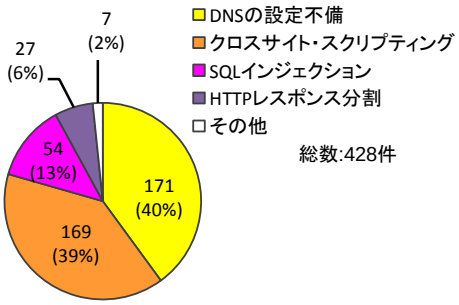


図9.重要インフラのウェブサイトの
脆弱性の種類(2009年第1四半期)

2.4 DNS キャッシュポイズニングの脆弱性の届出が継続

図 10 は DNS キャッシュポイズニング脆弱性の月別の届出件数と 3 月末現在の対策状況です。2008 年 4 月から 2009 年 3 月まで（2008 年度）の届出の累計は 1,131 件で、216 件は取扱い終了（ウェブサイトが修正完了）しましたが、現時点で取扱い中（ウェブサイトが対策中）のものが 915 件あります。

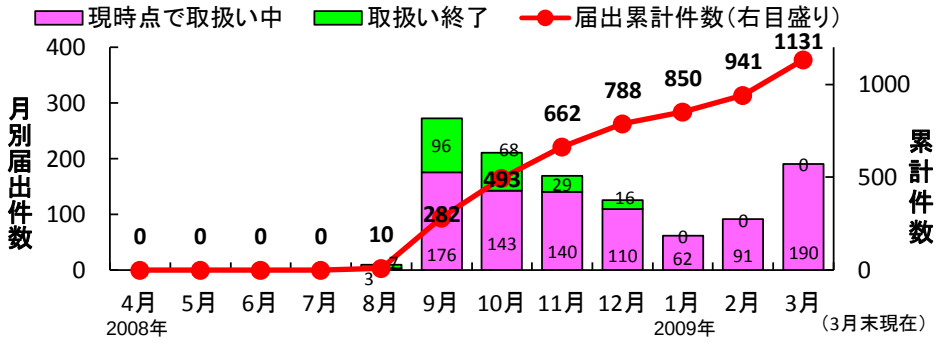


図10.DNSキャッシュポイズニング脆弱性の届出件数と対策状況

[13]「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」:
http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html

2.5 クロスサイト・スクリプティング脆弱性の届出が継続

図 11 はクロスサイト･スクリプティング脆弱性の月別の届出件数と 3 月末現在の対策状況です。2008 年度の届出の累計は 1,225 件で、217 件は取扱い終了（ウェブサイトが修正完了）しましたが、現時点で取扱い中（ウェブサイトが対策中）のものが 1,008 件あります。

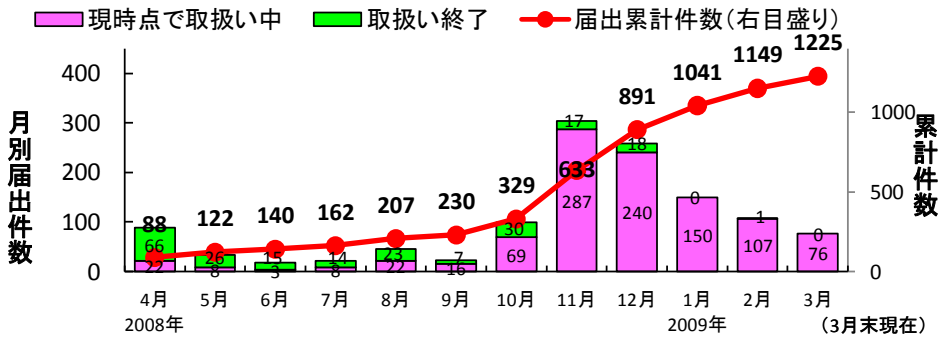


図11.クロスサイト･スクリプティング脆弱性の届出件数と対策状況

2.6 SQL インジェクション脆弱性の届出が継続

図 12 は SQL インジェクション脆弱性の月別の届出件数と 3 月末現在の対策状況です。2008 年度の届出の累計は 318 件で、43 件は取扱い終了（ウェブサイトが修正完了）しましたが、現時点で取扱い中（ウェブサイトが対策中）のものが 275 件あります。

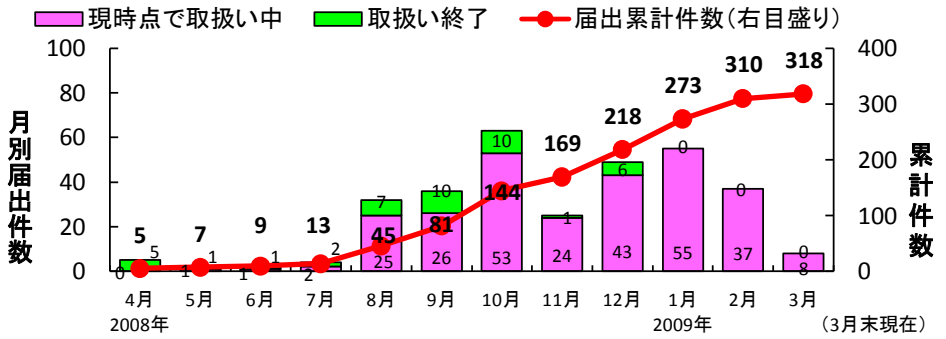


図12.SQLインジェクション脆弱性の届出件数と対策状況

2.7 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 592 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 13 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 369 件、200 日から 299 日のものは 74 件などとなっており、これらの合計は 592 件（前四半期は 258 件）となりました。前四半期のものは 35 件減少しましたが、今四半期で新たに 369 件が 90 日以上となったため、334 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。**

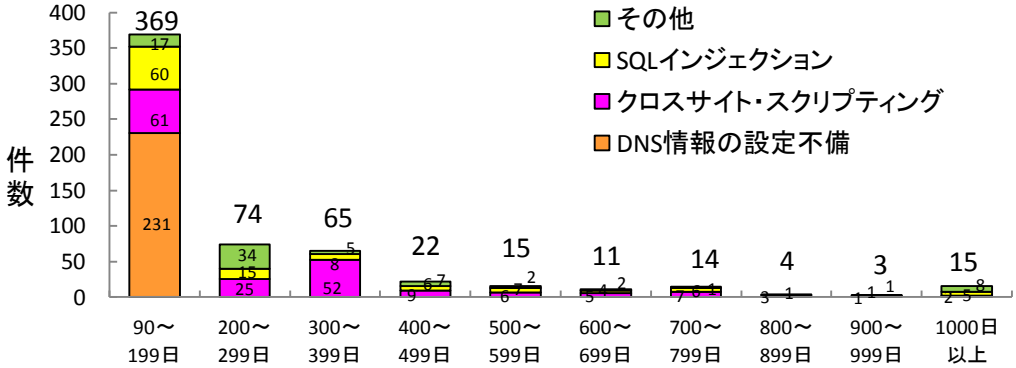


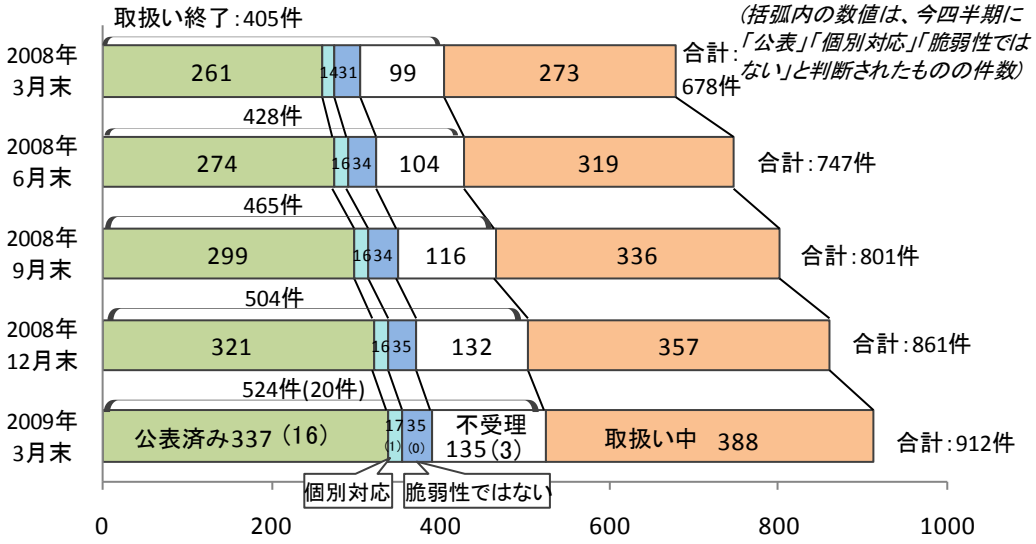
図13. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

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 337 件）です。また、「製品開発者が個別対応」したものは 1 件（累計 17 件）、「不受理」としたものは 3 件（累計 135 件）、取扱中は 388 件です。



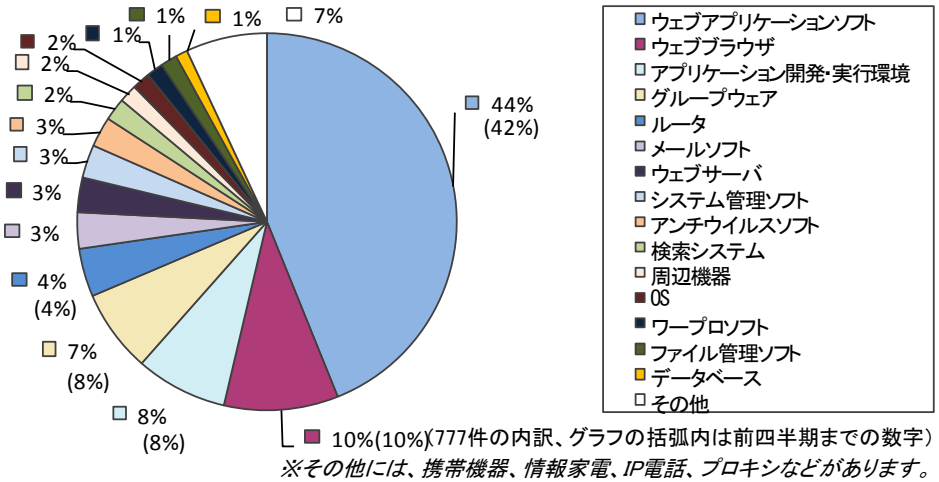
公表済み:	JVN で脆弱性への対応状況を公表したもの
個別対応:	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない:	製品開発者により脆弱性ではないと判断されたもの
不受理:	告示で定める届出の対象に該当しないもの
取扱い中:	製品開発者が調査、対応中のもの

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 912 件のうち、不受理のものを除いた 777 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。



（777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、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2009年3月末まで）

届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 912 件のうち、不受理のものを除いた 777 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 14 件ありました。

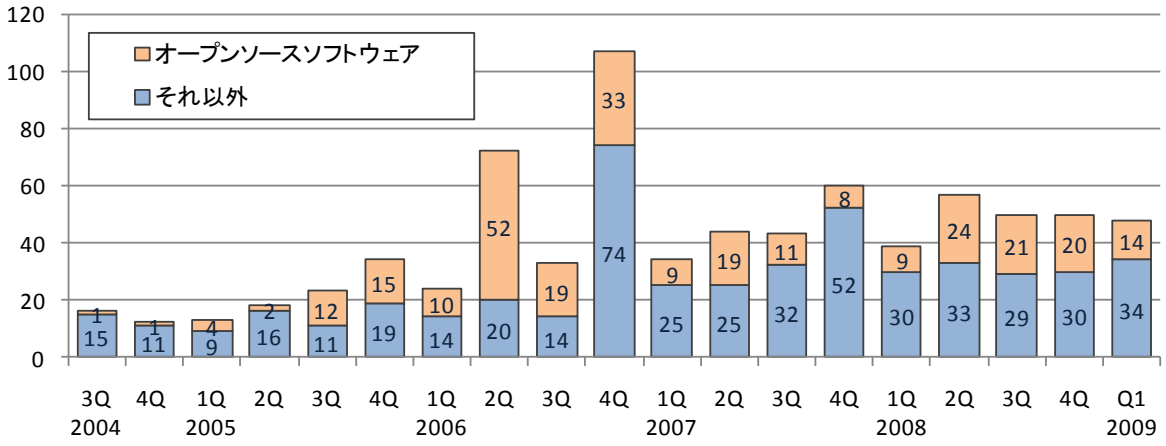
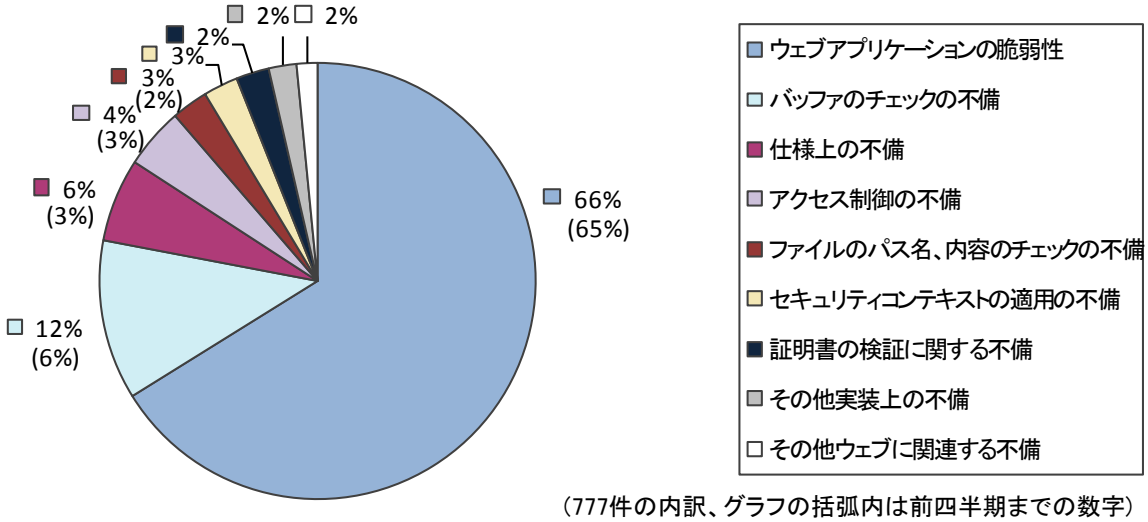


図1-3.オープンソースソフトウェアの脆弱性の届出件数　（777件の内訳）

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 912 件のうち、不受理のものを除いた 777 件の原因別[14]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。



（777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3月末まで）

[14] 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。

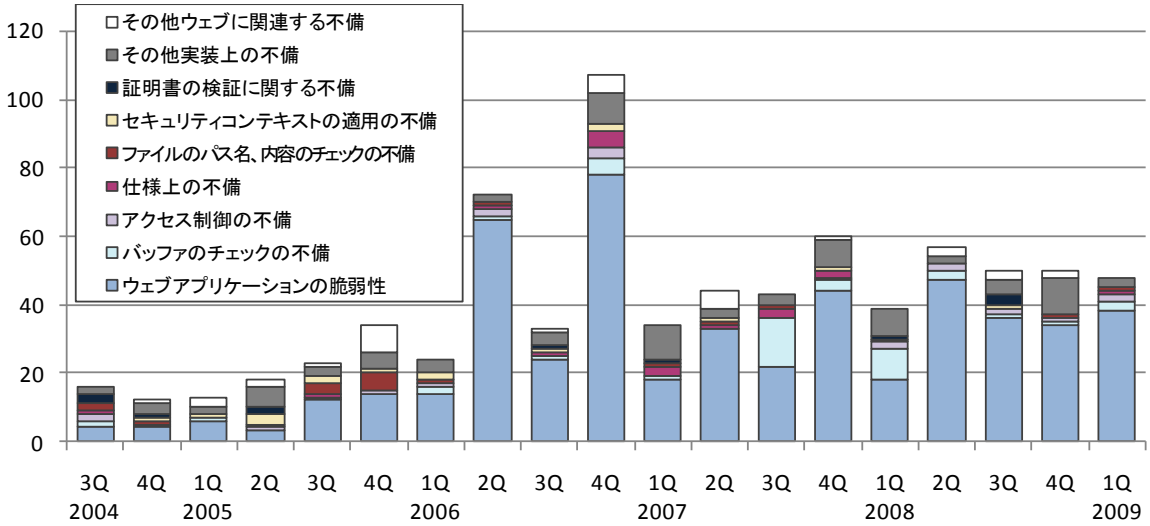
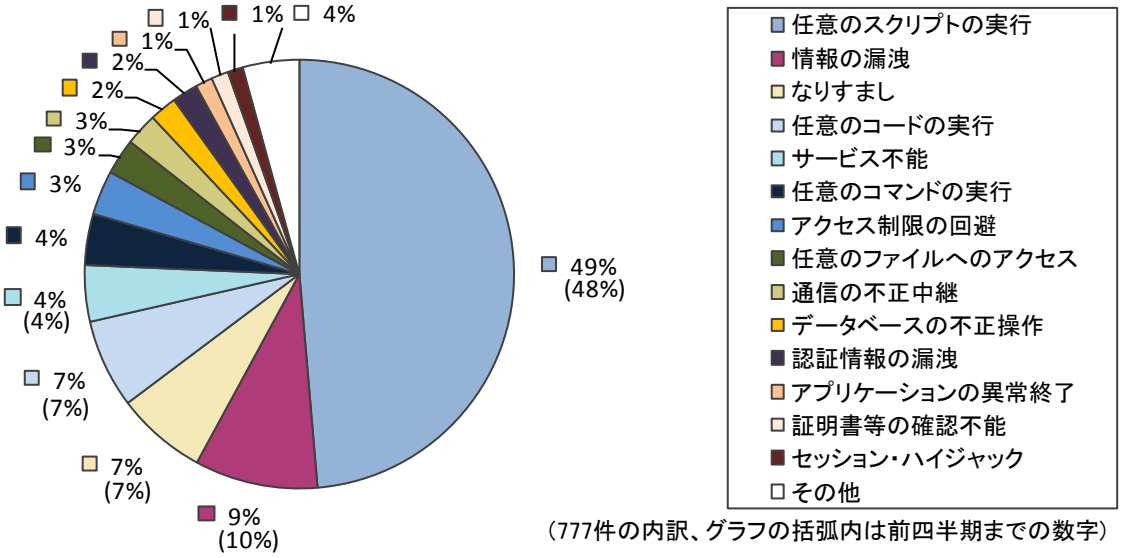


図1-5. ソフトウェア製品の脆弱性 原因別件数の推移（届出受付開始から2009年3月末まで）



（777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[15] 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	16 件	337 件
②	海外 CSIRT 等と連携して公表したもの	15 件	407 件
	計	31 件	744 件

[15] 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 3 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 33%であり、公表するまでに要した日数は 2008 年第 2 四半期からほぼ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。

45 日以内の公表件数の割合

2008/3Q まで	2008/4Q まで	2009/1Q まで
32%	32%	33%

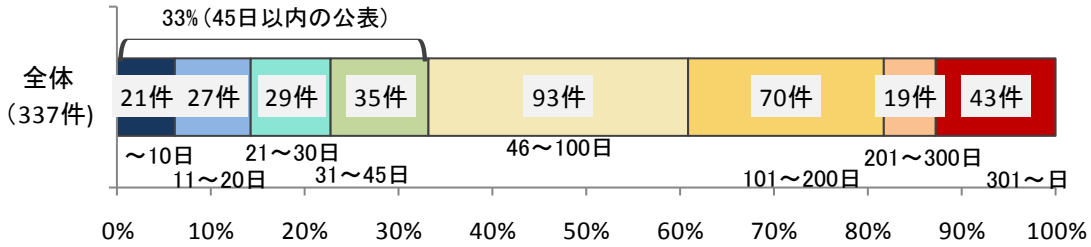


図1-7. ソフトウェア製品の脆弱性公表日数

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 2 件（表 1-2 の*2）、組込みソフトウェア製品の脆弱性が 2 件（表 1-2 の*3）ありました。

表 1-2.2009 年第 1 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.				
1	futomi's CGI Cafe 製「全文検索 CGI」における管理者権限奪取の脆弱性	ウェブサイト用検索ソフト「全文検索 CGI」には、管理者権限が奪取可能である脆弱性がありました。 このため、第三者により全文検索 CGI の管理者になりすまされる可能性がありました。	2009 年 1 月 23 日	7.5
2	futomi's CGI Cafe 製「MP Form Mail CGI」における管理者権限奪取の脆弱性	メールフォームソフト「MP Form Mail CGI」には、管理者権限が奪取可能である脆弱性がありました。 このため、第三者により MP Form Mail CGI の管理者になりすまされる可能性がありました。	2009 年 3 月 10 日	7.5
3	futomi's CGI Cafe 製「高機能アクセス解析 CGI Professional 版」における管理者権限奪取の脆弱性	アクセス解析ソフト「高機能アクセス解析 CGI Professional 版」には、管理者権限が奪取可能である脆弱性がありました。 このため、第三者により高機能アクセス解析 CGI Professional 版の管理者になりすまされる可能性がありました。	2009 年 3 月 31 日	7.5

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				
4	「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」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 1 月 8 日	4.3
5 (*1)	「MODx」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「MODx」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 1 月 9 日	4.3
6 (*1)	「MODx」における SQL インジェクションの脆弱性	コンテンツ管理システム「MODx」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 1 月 9 日	5.1
7 (*3)	「Cisco IOS」におけるクロスサイト・スクリプティングの脆弱性	シスコシステムズ社のネットワーク製品に搭載されている「Cisco IOS」のウェブ管理インターフェースには、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 1 月 15 日	4.3
8	「Becky! Internet Mail」におけるバッファオーバーフローの脆弱性	メールクライアントソフト「Becky! Internet Mail」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 2 月 12 日	6.8
9 (*2) (*3)	ソニー製ネットワークカメラ SNC シリーズの 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	ソニー製ネットワークカメラ SNC シリーズの ActiveX コントロールには、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 2 月 23 日	6.8
10 (*1)	PEAK XOOPS 製「piCal」におけるクロスサイト・スクリプティングの脆弱性	XOOPS 用スケジューラ付カレンダーモジュール「piCal」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 2 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
11	futomi's CGI Cafe 製「高機能アクセス解析 CGI Standard 版(Ver. 3.x 系) 」におけるクロスサイト・スクリプティングの脆弱性	アクセス解析ソフト「高機能アクセス解析 CGI Standard 版(Ver. 3.x 系) 」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 3 月 16 日	4.3
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
12 (*1) (*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 構築ソフト「MyNETS」には、ウェブページを出力する際の処理に問題がありました。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。	2009 年 1 月 7 日	3.5
13 (*1)	「MODx」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「MODx」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 MODx のコンテンツが編集される可能性がありました。	2009 年 1 月 9 日	2.6
14	「Oracle WebLogic 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 WebLogic Server」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 1 月 20 日	2.6
15	「FAST ESP」におけるクロスサイト・スクリプティングの脆弱性	検索プラットフォーム「FAST ESP」の管理画面には、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 2 月 10 日	2.6
16 (*1)	「Apache Tomcat」における情報漏えいの脆弱性	The Apache Software Foundation が提供する「Apache Tomcat」には、情報漏えいの脆弱性がありました。このため、第三者により別の利用者のリクエストデータに含まれるパスワード、セッション ID、ユーザ ID 等の情報が漏えいする可能性がありました。	2009 年 2 月 26 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 15 件には、通常の脆弱性情報 8 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[16]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	MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造	複数製品開発者へ通知
2	AREVA e-terra habitat に複数の脆弱性	注意喚起として掲載
3	GoAhead WebServer に情報漏えいの脆弱性	注意喚起として掲載
4	Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge に URL リダイレクションの脆弱性	注意喚起として掲載
5	Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
6	GE Fanuc Proficy HMI/SCADA iFIX の認証機能における脆弱性	注意喚起として掲載
7	透過型プロキシサーバが HTTP の Host ヘッダに依存して接続を行う問題	複数製品開発者へ通知
8	libpng が適切にエレメントポインタを初期化しない脆弱性	複数製品開発者へ通知

表 1-4.米国 US-CERT[17]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 SMB プロトコルの脆弱性に対するアップデート
2	Oracle 製品における複数の脆弱性に対するアップデート
3	Microsoft Windows 自動実行機能の無効化における注意点
4	Apple QuickTime 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 Reader および Acrobat における脆弱性
7	Microsoft 製品における複数の脆弱性に対するアップデート

[16] 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。
[17] 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

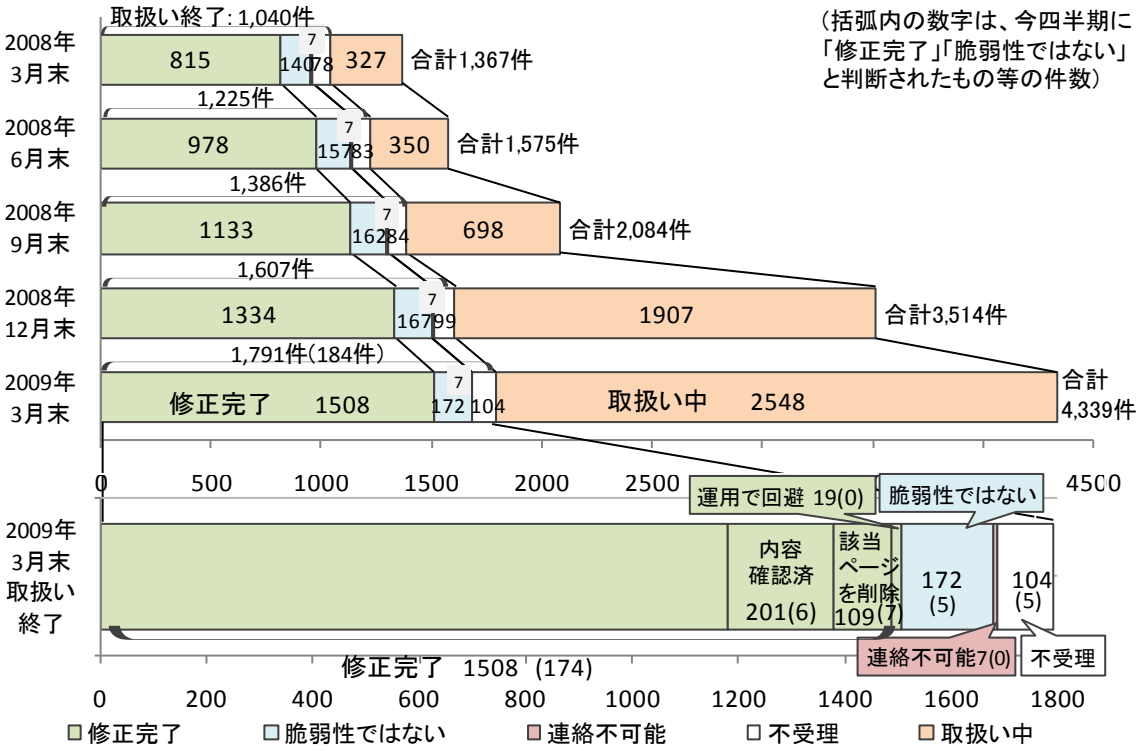
2.1 ウェブサイトの脆弱性の処理状況

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 184 件（累計 1,791 件）でした。このうち、「修正完了」したものは 174 件（累計 1,508 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 172 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 5 件（累計 104 件）でした。

取扱いを終了した累計 1,791 件のうち、「連絡不可能」「不受理」を除く累計 1,680 件（94%）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 6 件（累計 201 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 7 件（累計 109 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。

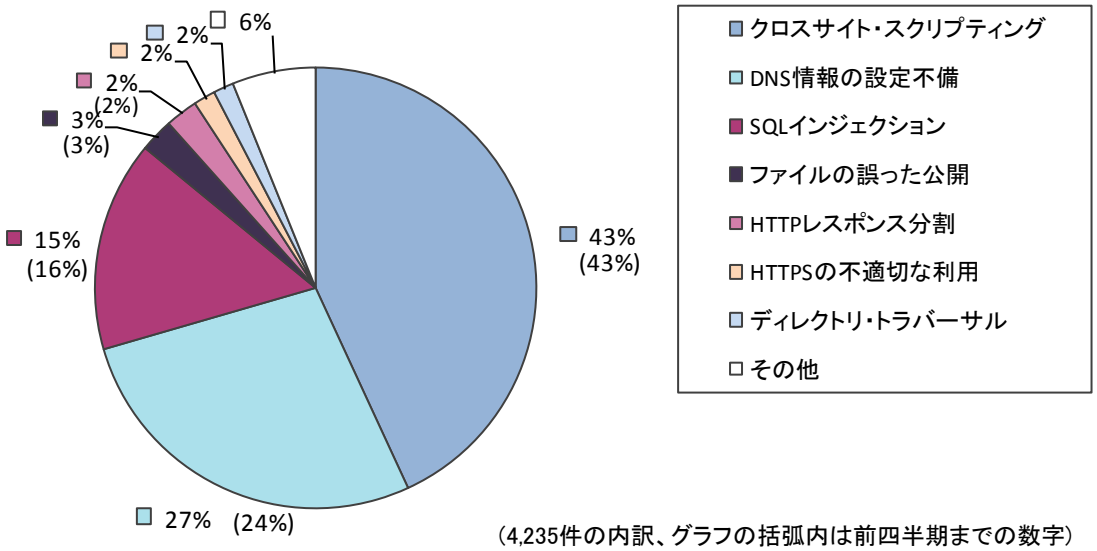


修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
内容確認済	：	修正完了のうち、IPA が修正を確認したもの
該当ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
運用で回避	：	修正完了のうち、運用により被害を回避しているもの
脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
不受理	：	告示で定める届出の対象に該当しないもの
取扱い中	：	ウェブサイト運営者が調査、対応中のもの

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 4,339 件のうち、不受理のものを除いた 4,235 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[18]。



（4,235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3月末まで）

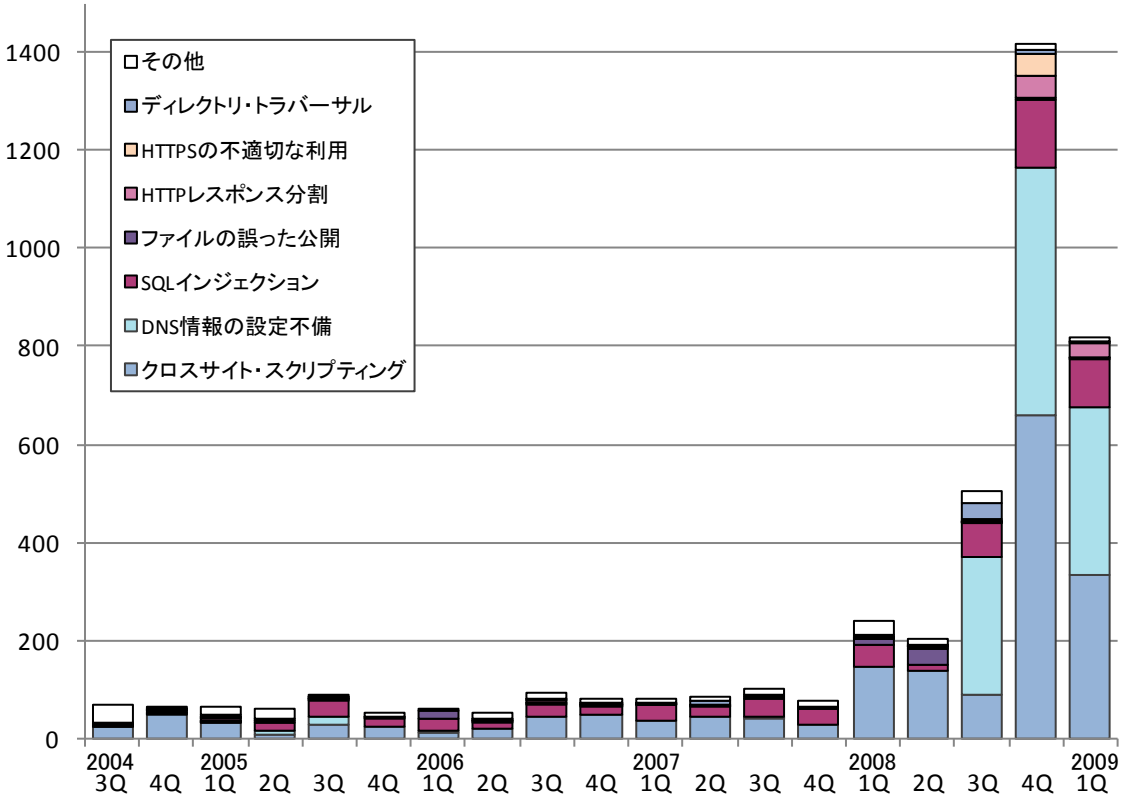
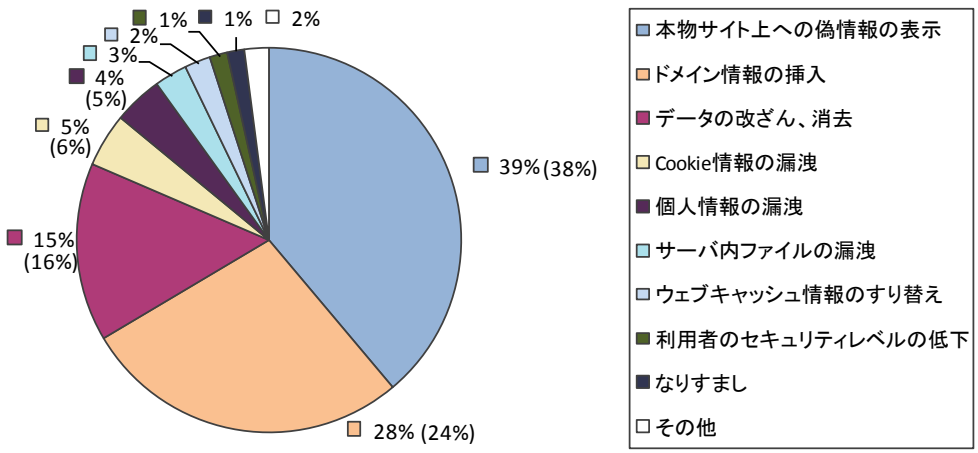


図2-3.ウェブサイトの脆弱性 種類別件数の推移（届出受付開始から2009年3月末まで）

[18] 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。



（4235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3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 85%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 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 2009 年 3 月末までの届出の中で、修正完了したものについて、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[19]。全体の 58%の届出が 30 日以内、全体の 80%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	2008/4 まで	2009/1Q まで
77%	81%	80%	83%	80%

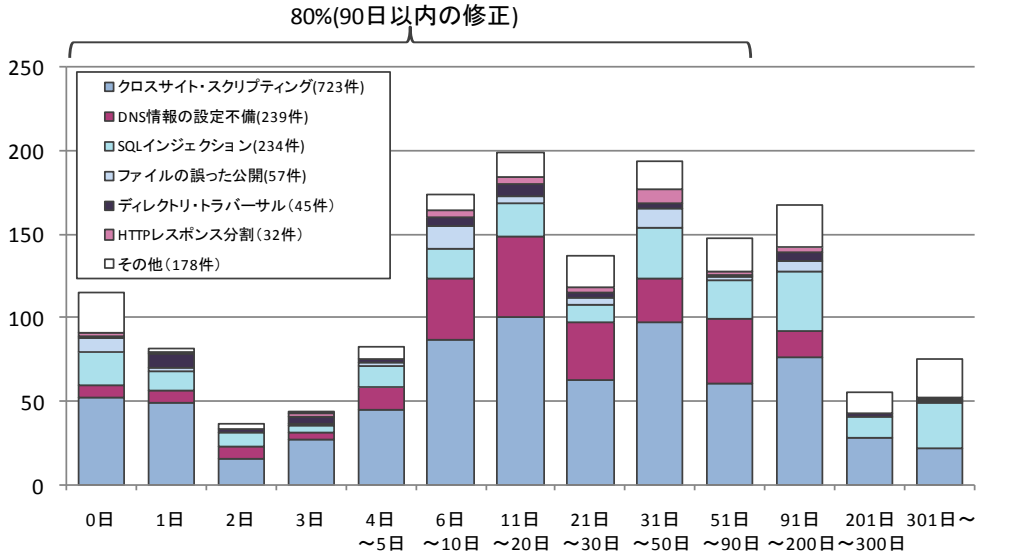


図2-5.ウェブサイトの修正に要した日数

[19] 前四半期までは運営者から修正完了の報告があったもののみを示していましたが、今四半期より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。

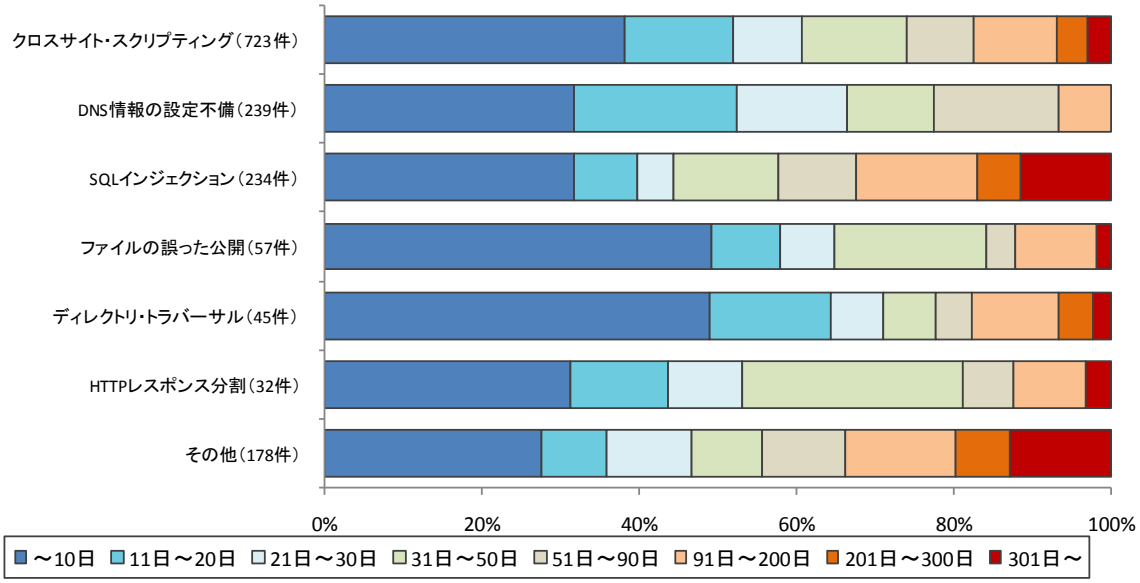


図2-6.ウェブサイトの修正に要した日数の傾向

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

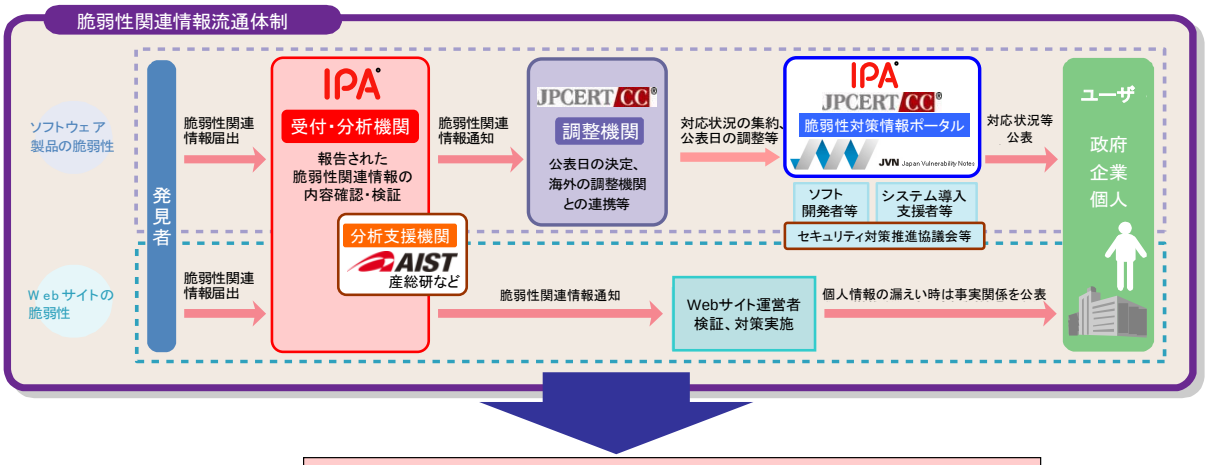
付表 2 ウェブサイト脆弱性の分類

	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