プレスリリース
2008 年 4 月 16 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 1 四半期(1 月～3 月)]

独立行政法人 情報処理推進機構(略称:IPA、理事長:西垣 浩司)および有限責任中間法人 JPCERT コーディネーションセンター(略称:JPCERT/CC、代表理事:歌代 和正)は、2008 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。

今四半期のトピックス:
「情報セキュリティ早期警戒パートナーシップ」による脆弱性の届出件数が 2,000 件に達しました。

1. 2008 年第 1 四半期の概況

1.1 脆弱性の届出状況

2008 年第 1 四半期(2008 年 1 月 1 日から 3 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 **53** 件、ウェブアプリケーション(ウェブサイト)に関するもの **244** 件、合計 **297** 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 **679** 件、ウェブサイトに関するもの **1,367** 件、合計 **2,046** 件で、ウェブサイトに関する届出が全体の 3 分の 2 を占めています(表1)。

表 1. 2008 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	53 件	679 件
ウェブサイト	244 件	1,367 件
計	297 件	2,046 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 **2.24** 件となりました。**累計件数が 1,000 件に達するのに 2 年半(2004 年 3Q～2006 年 4Q)を要しましたが、その後、1 年 3 カ月(2007 年 1Q～2008 年 1Q)で 2,000 件に達しました**(図 1)。

今四半期は、政府機関のウェブサイトに関する脆弱性や、特定のウェブブラウザの動作に依存したウェブサイトの脆弱性の届出が増加するなど、ウェブサイトに関する届出が過去最多を記録しました。**これまで見落とされがちだったものが多数届出られ、潜在していた脆弱性が顕在化しているものと考えています。**

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)

2005/1Q	2006/1Q	2006/2Q	2006/3Q	2006/4Q	2007/1Q	2007/2Q	2007/3Q	2007/4Q	2008/1Q
1.45	1.61	1.70	1.75	1.92	1.95	1.98	2.03	2.05	2.24

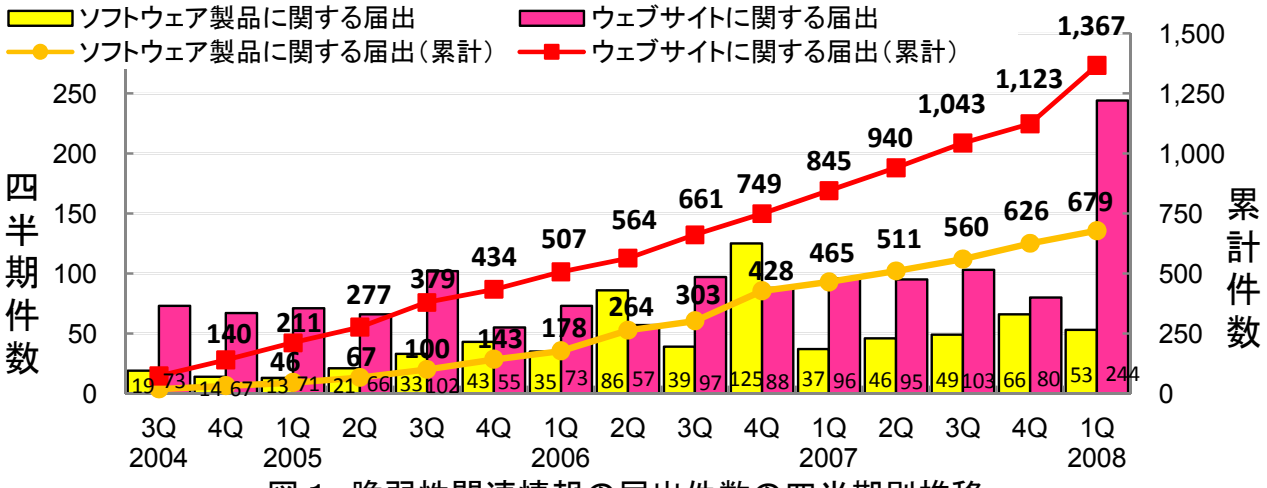


図 1. 脆弱性関連情報の届出件数の四半期別推移

[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。

1.2 脆弱性の取扱い状況

2008 年第 1 四半期の脆弱性の取扱い状況は、ソフトウェア製品に関して届出が **53** 件あり、取扱い終了[2]が **33** 件のため、取扱中が **20** 件増加して累計 **274** 件となりました。ウェブサイトに関しては、届出が **244** 件あり、取扱い終了[3]が **78** 件のため、取扱中が **166** 件増加して累計 **327** 件となりました(表 2)。

表 2. 2008 年第 1 四半期の取扱い件数

分類	状況	件数	累計件数
ソフトウェア製品	届出	53 件	679 件
	取扱い終了	33 件	405 件
	取扱い中	20 件	274 件
ウェブサイト	届出	244 件	1,367 件
	取扱い終了	78 件	1,040 件
	取扱い中	166 件	327 件

図 2 は、ソフトウェア製品に関して各四半期に届出のあったものの現在の取扱い状況です。例えば、2006 年第 2 四半期に届出のあった 86 件は、50 件の取扱いを終了しましたが 36 件は取扱中です。また、2006 年第 3 四半期に届出のあった 39 件は、23 件の取扱いを終了しましたが 16 件は取扱中です。

このように、**ソフトウェア製品に関しては、2006 年に届出られたものでも、まだ、38%が取扱中のままです。2007 年に届出られたものの 56%が取扱中のままです。ソフトウェア製品開発者は、脆弱性を攻撃された場合の顧客システムへの影響の重大さを認識し、早期に対策を講じる必要があります。**

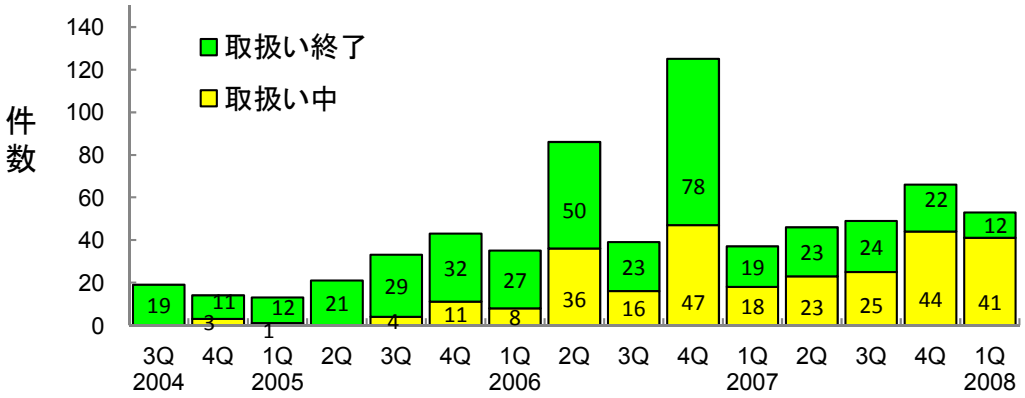


図2. ソフトウェア製品に関して各四半期に届出のあったものの現在の状況

ウェブサイトに関しては 2007 年に届出られたものの 24%が取扱い中のままです(図 3)。ウェブサイト運営者は、脆弱性を攻撃された場合の重大さを認識し、早期に対策を講じる必要があります。

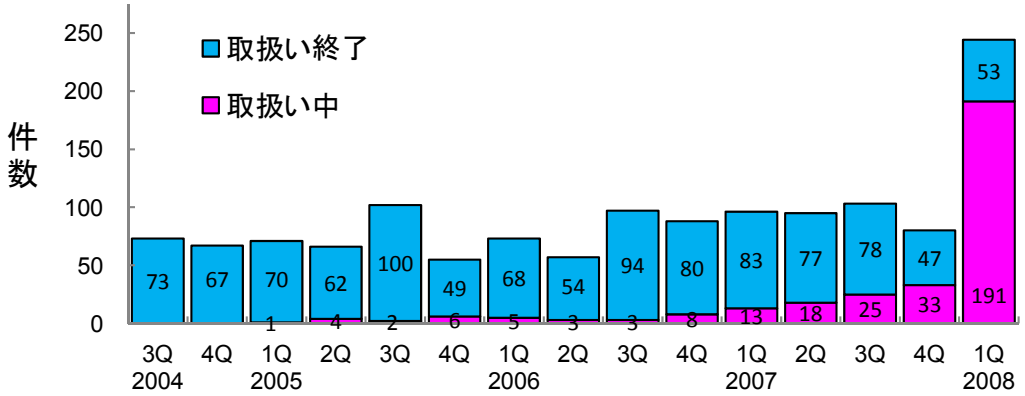


図3. ウェブサイトに関して各四半期に届出のあったものの現在の状況

[2] ソフトウェア製品開発者が修正完了したもの、脆弱性ではないと判断したもの、不受理のもの。
[3] ウェブサイト運営者が修正完了したもの、脆弱性ではないと判断したもの、連絡不可能なもの、不受理のもの。

2.ソフトウェア製品の脆弱性の処理状況

2008 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[4]で対策情報を公表したものは **19** 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 **2** 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 **12** 件でした。これらの取扱いを終了したものの合計は **33** 件（累計 **405** 件）です（表 3）。

表 3. 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	19 件	261 件
	個別対応	2 件	14 件
脆弱性ではない		0 件	31 件
不受理		12 件	99 件
合計		33 件	405 件

この他、海外の CSIRT[5]から JPCERT/CC が連絡を受けた **24** 件（累計 **327** 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。

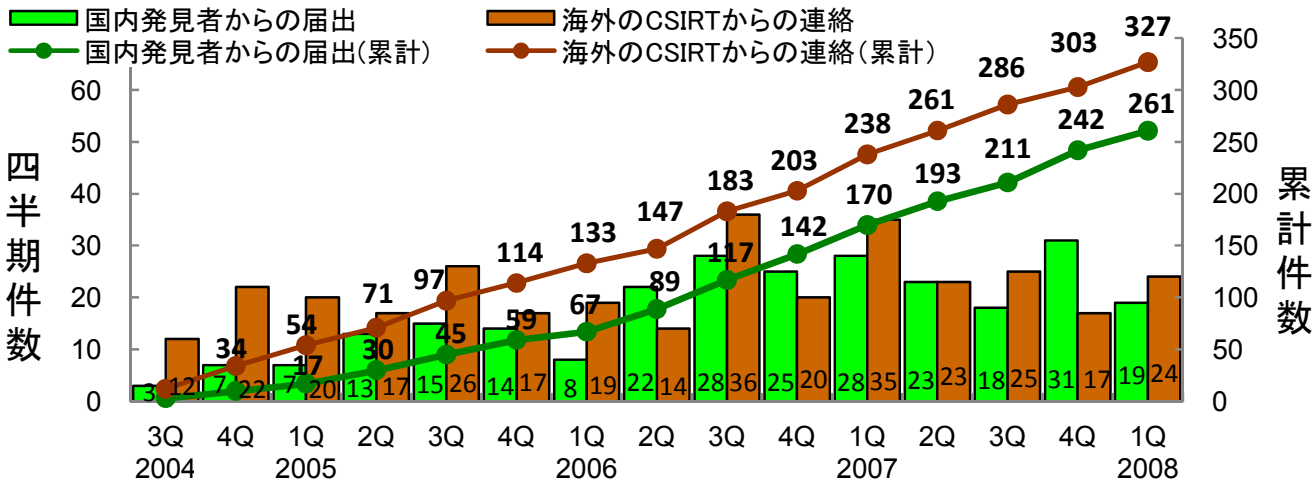


図 4．ソフトウェア製品の脆弱性対策情報の公表件数

なお、2008 年第 1 四半期において、JVN で対策情報を公表した主なものは、以下のとおりです。

(1)「アイ・オー・データ製無線 LAN ルータ」の脆弱性[6]

ネットワーク機器の「アイ・オー・データ製無線 LAN ルータ」に組込まれたソフトウェアに、認証機能が初期設定で無効となっている脆弱性が存在しました。この脆弱性が悪用されると外部から管理画面を操作されてしまう可能性があり、3 月 18 日に JVN で対策情報を公表しました。

(2)「Sun JRE」の脆弱性[7]

Java プログラムを実行するためのソフトウェア「Sun JRE (Java Runtime Environment)」に、本来権限が無いと実行できない処理を誤って実行してしまう脆弱性が存在しました。この脆弱性が悪用されると、ローカルファイルなどにアクセスされてしまう可能性があり、3 月 11 日に JVN で対策情報を公表しました。

---

[4] 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/

[5] 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。

[6] 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 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=6.8、別紙 P.6 表 1-2 項番 14 を参照下さい。

(3)「ジャストシステム製品」の脆弱性[8]

日本語ワープロソフトウェアや表計算ソフトウェアなどの「ジャストシステム製品」のファイルを読みこむ処理に、バッファオーバーフローの脆弱性が存在し、ウェブブラウザの種類によっては、悪意のある URL にアクセスするだけで被害を受ける可能性がありました。

この脆弱性が悪用されると、システムが破壊されたり、ウイルスやボットに感染させられたりしてしまう可能性があり、1 月 7 日に JVN で対策情報を公表しました。

(4)「ヤマハルーター製品」の脆弱性[9]

ネットワーク機器の「ヤマハルーター製品」に組込まれたソフトウェアに、クロスサイト・リクエスト・フォージェリ(CSRF)の脆弱性があり、1 月 28 日に JVN で対策情報を公表しました。

組込みソフトウェアの脆弱性は、今四半期は(1)(4)の他に「複数のキヤノン製デジタル複合機およびレーザービームプリンターの脆弱性」[10]の計 3 件の脆弱性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 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 **67** 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 **9** 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 **2** 件でした。これらの取扱いを終了したものの合計は **78** 件(累計 **1,040** 件)です(表 4)。

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 4. 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	67 件	815 件
脆弱性ではない	9 件	140 件
連絡不可能	0 件	7 件
不受理	2 件	78 件
合計	78 件	1040 件

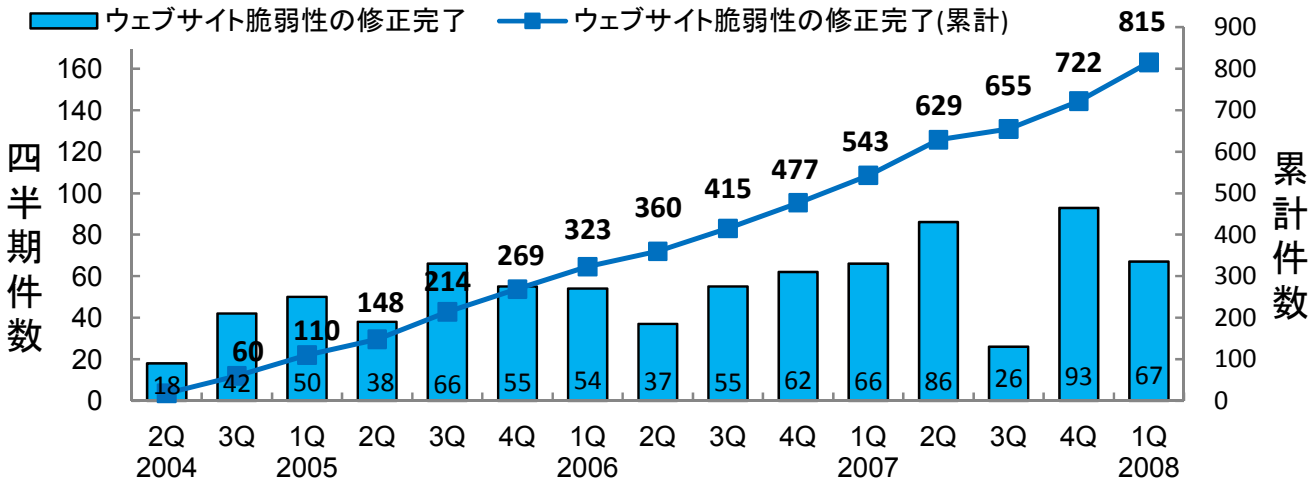


図 5. ウェブサイトの脆弱性の修正完了件数

[8] 本脆弱性の深刻度=レベル II(警告)、CVSS 基本値=6.8、別紙 P.4 表 1-2 項番 2 を参照下さい。
[9] 本脆弱性の深刻度=レベル II(警告)、CVSS 基本値=4.0、別紙 P.4 表 1-2 項番 3 を参照下さい。
[10] 本脆弱性の深刻度=レベル II(警告)、CVSS 基本値=5.0、別紙 P.5 表 1-2 項番 11 を参照下さい。

3.1 運営主体の内訳～政府機関のウェブサイトに関して通常より多数の届出

届出受付開始(2004 年 7 月 8 日)からの今四半期までに届出を受付けたウェブサイトの運営主体別内訳は、企業合計が 71%、政府機関が 6%、地方公共団体が 7%、団体(協会・社団法人)が 9%、教育・学術機関が 4%、個人が 6%となっています(図 6)。

今四半期のみを見ると、政府機関のウェブサイトに関する届出が 13%あり、通常の倍の割合の届出となっています(図 7)。

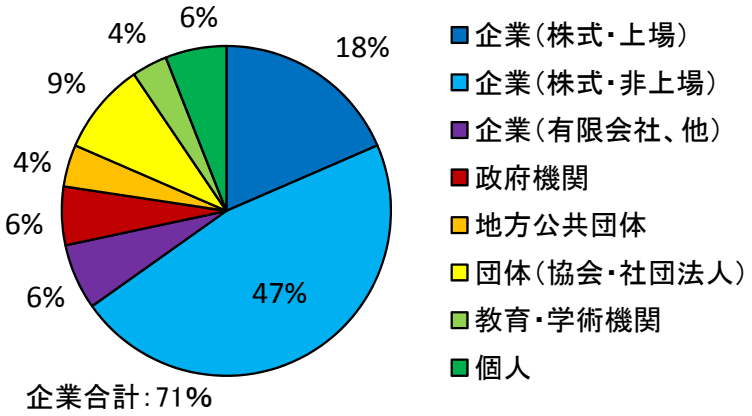


図6.ウェブサイトの運営主体(届出受付開始からの累計)

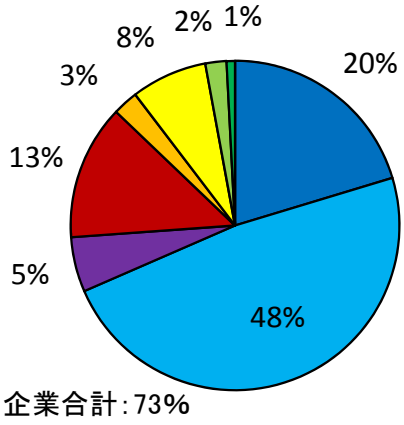


図7.ウェブサイトの運営主体(今四半期のみ)

3.2 特定のウェブブラウザの動作に依存したウェブサイトの脆弱性の届出が多数

今四半期は、特定のウェブブラウザの動作に依存したウェブサイトのクロスサイト・スクリプティングの脆弱性の届出が多くありました(図 8)。これは、ウェブサイトが文字コードを指定しない場合におけるウェブブラウザの文字コードの解釈に関するもの(UTF-7)や、スクリプトに該当する文字列(Internet Explorer の expression プロパティ)に関するものです。クロスサイト・スクリプティング対策をしていても、対策が不十分なウェブサイトが多く見うけられます。

ウェブサイトの開発者は「ウェブブラウザが文字コードを独自に解釈することがないように明示的な文字コードの指定を行う」[11]、「入力された HTML テキストから、スクリプトに該当する文字列を排除する」[12]などの対策が必要です。

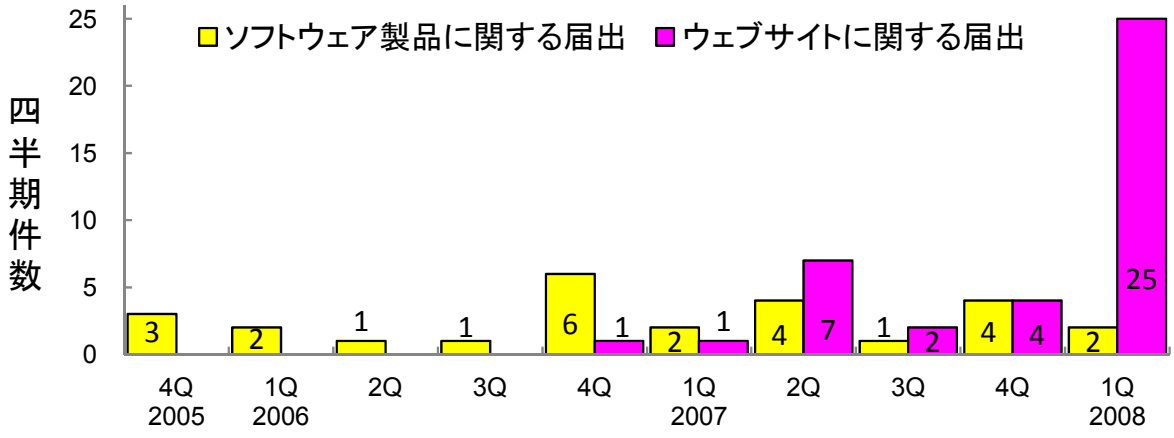


図8. 特定のウェブブラウザの動作に依存した脆弱性の届出件数

[11] 「安全なウェブサイトの作り方 改訂第 3 版」P.25 の 8)を参照。
[12] 「安全なウェブサイトの作り方 改訂第 3 版」P.25 の 7)を参照。

3.3 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 108 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。また、今四半期は、特に修正が長期化しているウェブサイト運営者に面会するなど、更に脆弱性対策を促しました。

この結果、ウェブサイトの脆弱性で 90 日以上も対策が完了していないものは、前四半期から **21** 件減少しました。しかし、今四半期で新たに **34** 件が 90 日以上となったため、**13** 件増加し累計で **108** 件（前四半期は **95** 件）となりました。また、300 日以上も対策が完了していないものが **14** 件増加し累計で **53** 件（前四半期は **39** 件）となりました（図 9）。

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。**

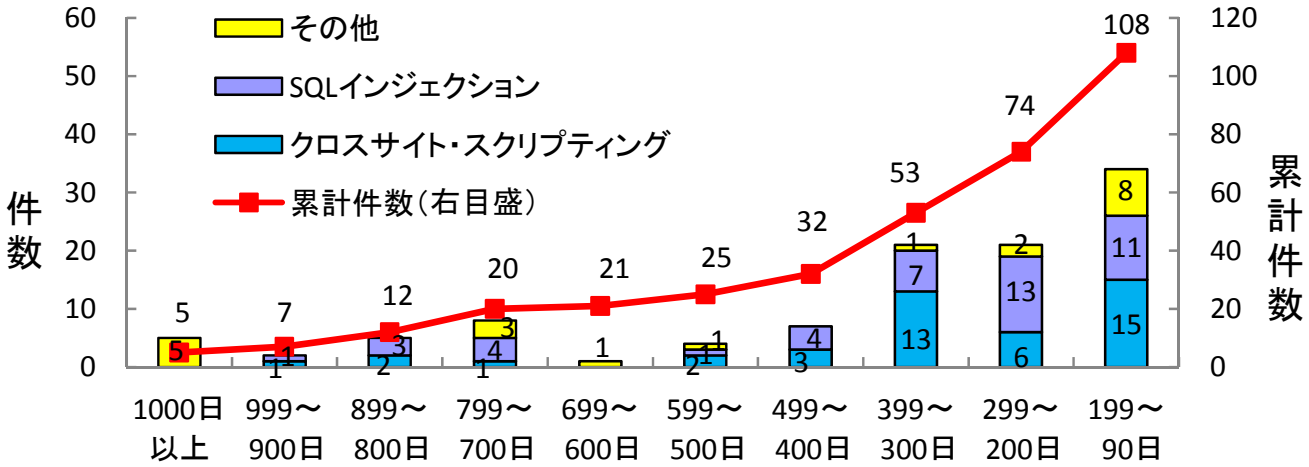


図9. 修正が長期化しているウェブサイトの未修正の経過日数と脆弱性の種類

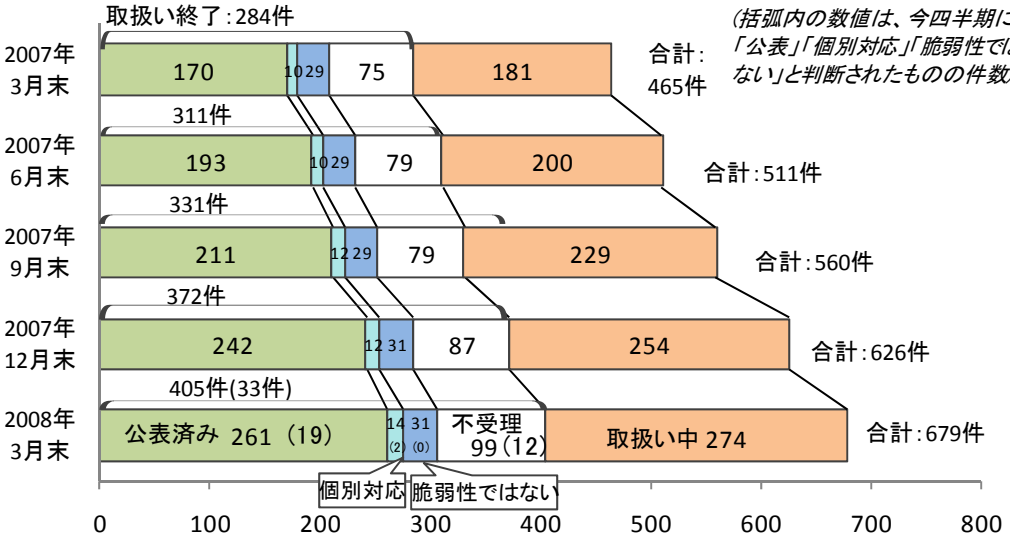
■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター 情報流通対策グループ 古田
Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: office@jpcert.or.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター 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、**19** 件（累計 **261** 件）です。また、「不受理」としたものは **12** 件（累計 **99** 件）です。



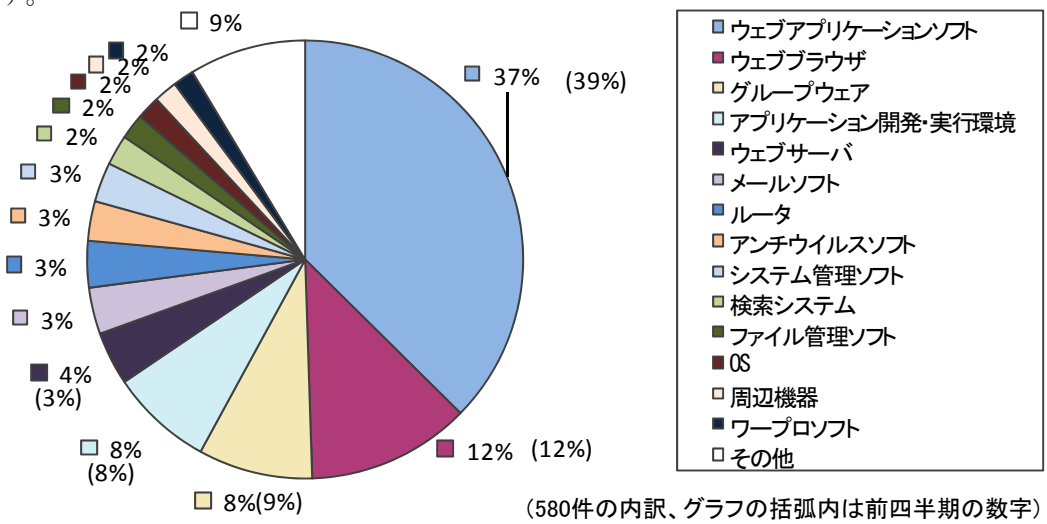
公表済み:	JVN で脆弱性への対応状況を公表したもの
個別対応:	製品開発者からの届出のうち、製品開発者が個別対応したもの
脆弱性ではない:	製品開発者により脆弱性ではないと判断されたもの
不受理:	告示で定める届出の対象に該当しないもの
取扱い中:	製品開発者が調査、対応中のもの

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 **679** 件のうち、不受理のものを除いた **580** 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。



（580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、データベース、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3月末まで）

図 1-3 に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増加し、今四半期も 11 件の届出がありました。

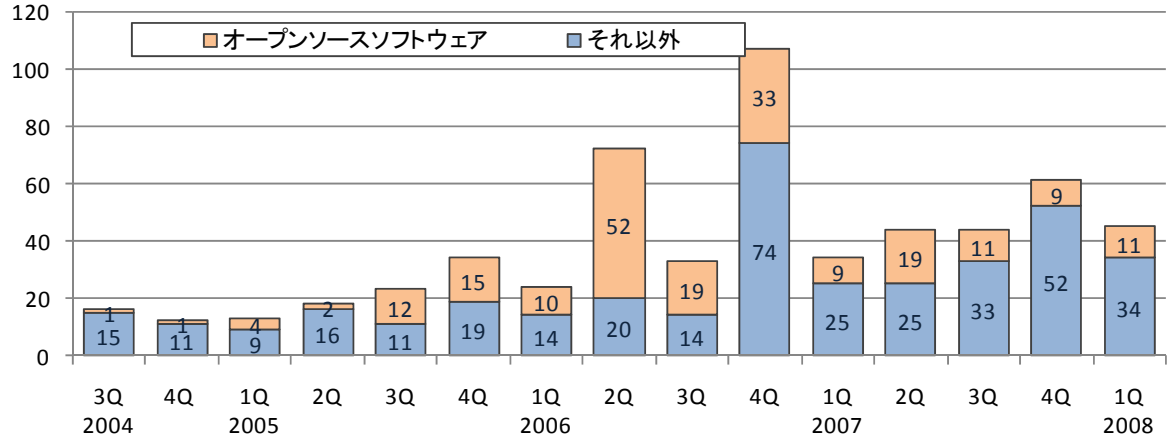
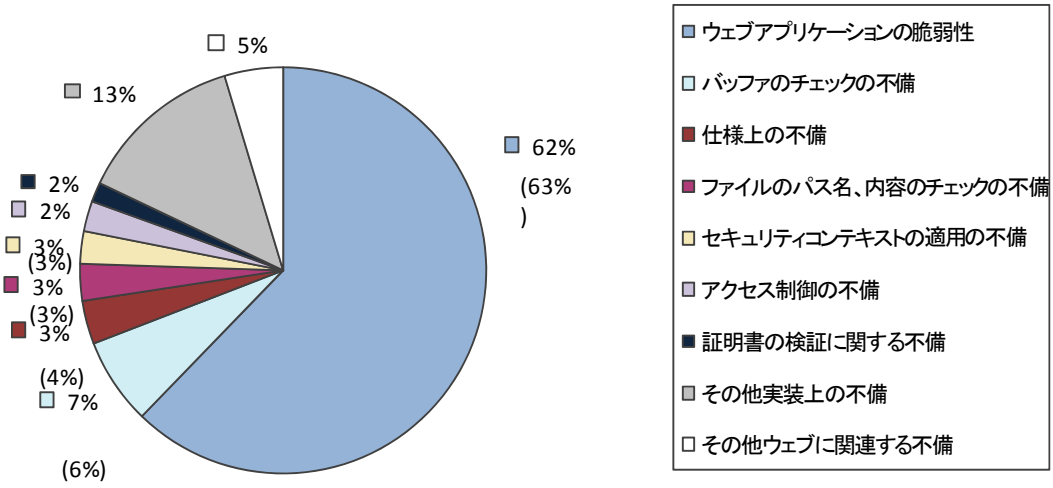


図1-3.オープンソースソフトウェアの脆弱性の届出件数 （580件の内訳）

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 **679** 件のうち、不受理のものを除いた **580** 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。



（580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3月末まで）

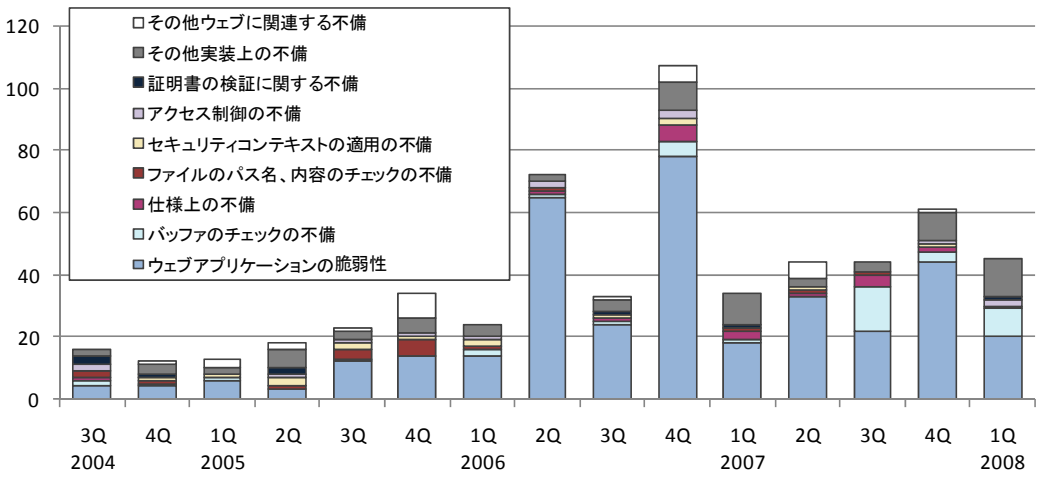
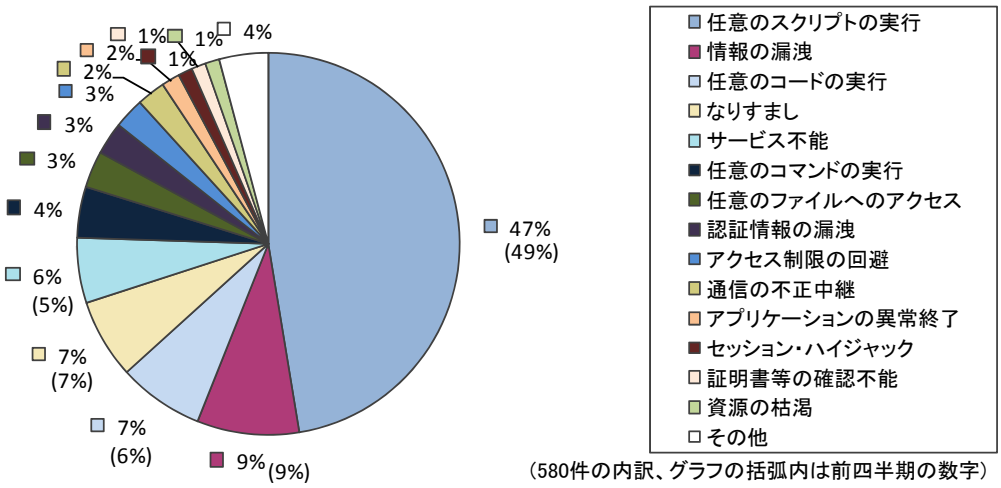


図1-5. ソフトウェア製品の脆弱性 原因別内訳（届出受付開始から2007年3月末まで）



（580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[13] 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	19 件	261 件
②	海外 CSIRT 等と連携して公表したもの	24 件	327 件
	計	43 件	588 件

[13] 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 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%と減少し、公表日数が増加する傾向にあります。製品開発者は脆弱性への早急な対応をお願いします。

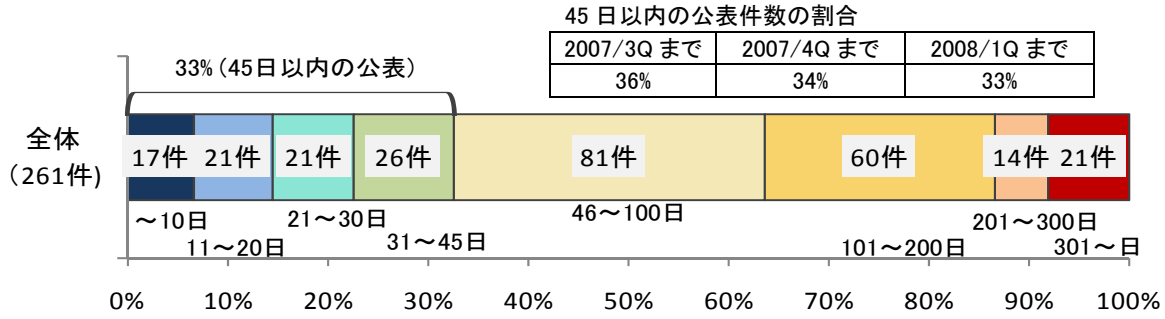


図1-7. ソフトウェア製品の脆弱性公表日数

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 4 件(表 1-2 の*1)、製品開発者自身から自社製品に関する脆弱性対策情報について連絡を受け公表したものが 2 件(表 1-2 の*2)、複数の製品開発者のソフトウェア製品に影響がある脆弱性が 1 件(表 1-2 の*3)あり、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 1-2.2008 年第 1 四半期に JVN で公表した脆弱性

項番	脆弱性	未対策状態での 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=7.0～10.0				
1 (*4)	アイ・オー・データ製無線 LAN ルータ WN-APG/R シリーズおよび WN-WAPG/R シリーズにおける初期設定に関する脆弱性	アイ・オー・データ製無線 LAN ルータ「WN-APG/R シリーズおよび WN-WAPG/R シリーズ」には、認証なしで管理画面を操作される脆弱性が存在しました。このため、第三者により当該製品の設定を変更されたり設定情報が読みだされる可能性がありました。	2008 年 3 月 18 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
2	複数のジャストシステム製品におけるバッファオーバーフローの脆弱性	ジャストシステムが提供する複数の製品には、バッファオーバーフローの脆弱性が存在しました。このため、ウェブサイトを閲覧するだけで、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。	2008 年 1 月 7 日	6.8
3 (*3) (*4)	複数のヤマハルーター製品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	ヤマハが提供する複数のルーター製品のウェブ設定画面には、クロスサイト・リクエスト・フォージェリの脆弱性が存在しました。ウェブ設定画面にログインした状態で悪意あるページにアクセスした場合、パスワードなどの設定が変更される可能性がありました	2008 年 1 月 28 日	4.0

項番	脆弱性	未対策状態での セキュリティ上の問題点	JVN 公表日	CVSS 基本値
4	複数の Hal Networks 製ショッピングカート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 Hal Networks 製ショッピングカート製品」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。	2008 年 1 月 28 日	4.3
5	「雷電 HTTPD」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバ「雷電 HTTPD」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 2 月 5 日	4.3
6	「PC2M」におけるクロスサイト・スクリプティングの脆弱性	携帯電話端末のウェブブラウザ向けにウェブページや画像などを閲覧できるように変換するソフト「PC2M」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 2 月 7 日	4.3
7 (*1)	「Apache Tomcat」において不正な Cookie を送信される脆弱性	The Apache Software Foundation が提供する「Apache Tomcat」には、不正な Cookie を送信される脆弱性が存在しました。このため、セッション・ハイジャックなどが行われる可能性がありました。	2008 年 2 月 12 日	4.3
8	「Internet Scanner」のレポート出力機能において任意のスクリプトが実行される脆弱性	脆弱性検査・監査ソフト「Internet Scanner」には、検査結果のレポートを出力する際の処理に問題がありました。このため、第三者により意図しないスクリプトが実行される可能性がありました。	2008 年 2 月 21 日	5.8
9	複数の Tor World 製 CGI スクリプトにおけるクロスサイト・スクリプティングの脆弱性	ウェブサイトの検索や掲示板などのソフトである「複数の Tor World 製 CGI スクリプト」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 2 月 21 日	4.3
10 (*1)	「Nagios」におけるクロスサイト・スクリプティングの脆弱性	稼働監視ソフト「Nagios」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 2 月 29 日	4.3
11 (*2) (*4)	複数のキヤノン製デジタル複合機、およびレーザービームプリンターにおいて不正なポートスキャンの中継が行われる脆弱性	「複数のキヤノン製デジタル複合機、およびレーザービームプリンター」には、FTP サーバ機能に問題がありました。このため、該当製品の FTP サーバ機能が他のネットワーク機器のポートスキャンに利用される可能性がありました。	2008 年 3 月 5 日	5.0
12 (*1)	「Zimbra Collaboration Suite」において任意のスクリプトが実行される脆弱性	予定表、アドレス帳およびウェブメール機能等を提供するウェブコラボレーションソフト「Zimbra Collaboration Suite」には、画像を表示する際の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 3 月 7 日	4.3

項番	脆弱性	未対策状態での セキュリティ上の問題点	JVN 公表日	CVSS 基本値
13	「BFup 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	ファイルのアップロード・ダウンロード機能の ActiveX コントロール「BFup 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存在しました。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。	2008 年 3 月 7 日	6.8
14	Sun JRE(Java Runtime Environment)の XSLT 処理における脆弱性	Java プログラムのソフトウェア実行環境「Sun JRE(Java Runtime Environment)」の XSLT 処理には、許可されている以上の権限で処理が行える脆弱性が存在しました。このため、第三者によりローカルファイルを閲覧されたり、任意のコードを実行されたり、不正終了によりウェブブラウザを終了されたりする可能性がありました。	2008 年 3 月 11 日	6.8
15 (*1) (*2)	「Namazu」におけるクロスサイト・スクリプティングの脆弱性	日本語全文検索ソフト「Namazu」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 3 月 21 日	4.3
16	「DesignForm」におけるクロスサイト・スクリプティングの脆弱性	メールフォームソフト「DesignForm」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 3 月 27 日	4.3
17	「PerlMailer」におけるクロスサイト・スクリプティングの脆弱性	メールフォームソフト「PerlMailer」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 3 月 27 日	4.3
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
18	「MTCMS ウィジウィグエディター」におけるクロスサイト・スクリプティングの脆弱性	ブログ管理ソフト「MTCMS ウィジウィグエディター」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 3 月 7 日	2.6
19	「Google デスクトップ」におけるクロスサイト・スクリプティングの脆弱性	コンピュータ内の情報検索ソフト「Google デスクトップ」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 3 月 12 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出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 24 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 12 件とが含まれます。これらの脆弱性情報は、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[14]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	Apple QuickTime RTSP の Response message に含まれる Reason-Phrase 処理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
2	Citrix Presentation Server 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
3	GE Fanuc Proficy Information Portal が任意のファイルをアップロードおよび実行を許可する問題	注意喚起として掲載
4	GE Fanuc CIMPLICITY HMI にヒープ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	GE Fanuc Proficy Information Portal が認証情報を平文で送信する問題	注意喚起として掲載
6	ネットワーク機器において UPnP が有効になっている場合の問題	複数製品開発者へ通知
7	Yahoo! Music Jukebox Yahoo! MediaGrid 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	注意喚起として掲載
8	Yahoo! Music Jukebox YMP Datagrid 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	注意喚起として掲載
9	KAME プロジェクトの IPv6 スタックにおける IPComp パケットの処理にサービス運用妨害(DoS)の脆弱性	複数製品開発者へ通知
10	Adobe Reader および Adobe Acrobat の JavaScript メソッド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
11	Samba send_mailslot() 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
12	Microsoft Jet Database Engine におけるバッファオーバーフローの脆弱性	緊急案件として掲載

表 1-4.米国 US-CERT[15]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	Apple Quicktime 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
5	Apple 製品における複数の脆弱性
6	Adobe Reader および Adobe Acrobat における脆弱性
7	Java における複数の脆弱性に対するアップデート
8	Microsoft 製品における複数の脆弱性に対するアップデート
9	MIT Kerberos の複数の脆弱性に対するアップデート
10	Apple 製品における複数の脆弱性に対するアップデート
11	Mozilla 製品における複数の脆弱性に対するアップデート
12	Cisco 製品における複数の脆弱性に対するアップデート

[14] CERT/Coordination Center。1998 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。

[15] 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

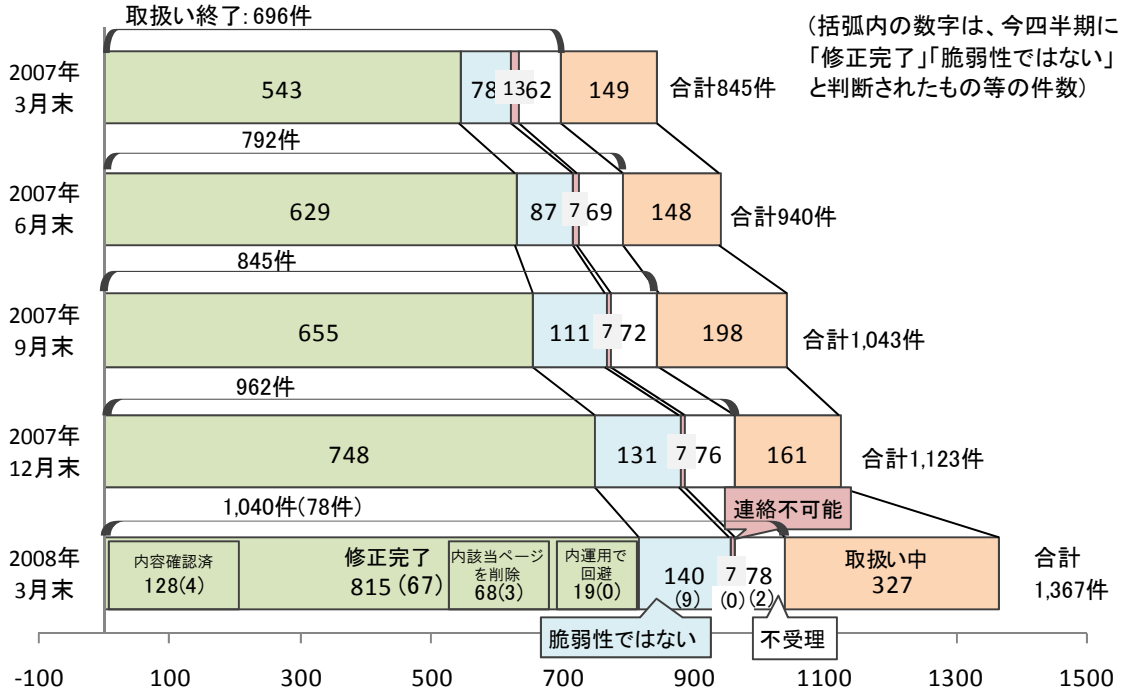
2.1 ウェブサイトの脆弱性の処理状況

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 **78** 件（累計 **1,040** 件）でした。このうち、「修正完了」したものは **67** 件（累計 **815** 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 **9** 件（累計 **140** 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 **2** 件（累計 **78** 件）でした。

取扱いを終了した累計 **1,040** 件のうち、「連絡不可能」「不受理」を除く累計 **955** 件（**92**%）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 **4** 件（累計 **128** 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 **3** 件（累計 **68** 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。



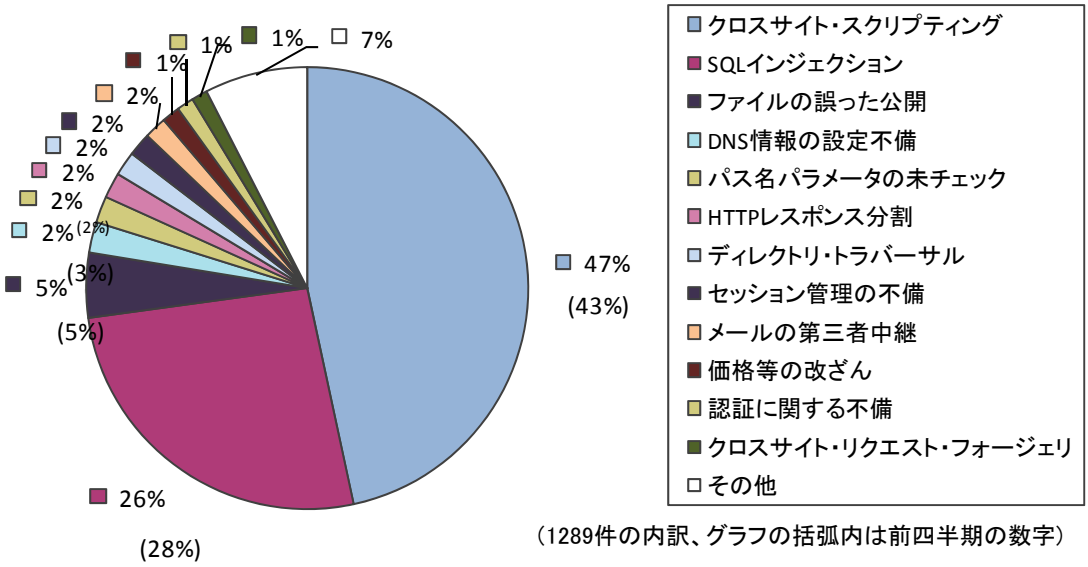
修正完了　：ウェブサイト運営者により脆弱性が修正されたもの
　確認済　：　修正完了のうち、IPA が修正を確認したもの
　当該ページを削除　：　修正完了のうち、当該ページを削除して対応したもの
　運用で回避　：　修正完了のうち、運用により被害を回避しているもの
脆弱性ではない　：ウェブサイト運営者により脆弱性はないと判断されたもの
連絡不可能　：ウェブサイト運営者からの回答がなく、取扱いができないもの
不受理　：告示で定める届出の対象に該当しないもの

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 **1,367** 件のうち、不受理のものを除いた **1,289** 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[16]。



（1289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）

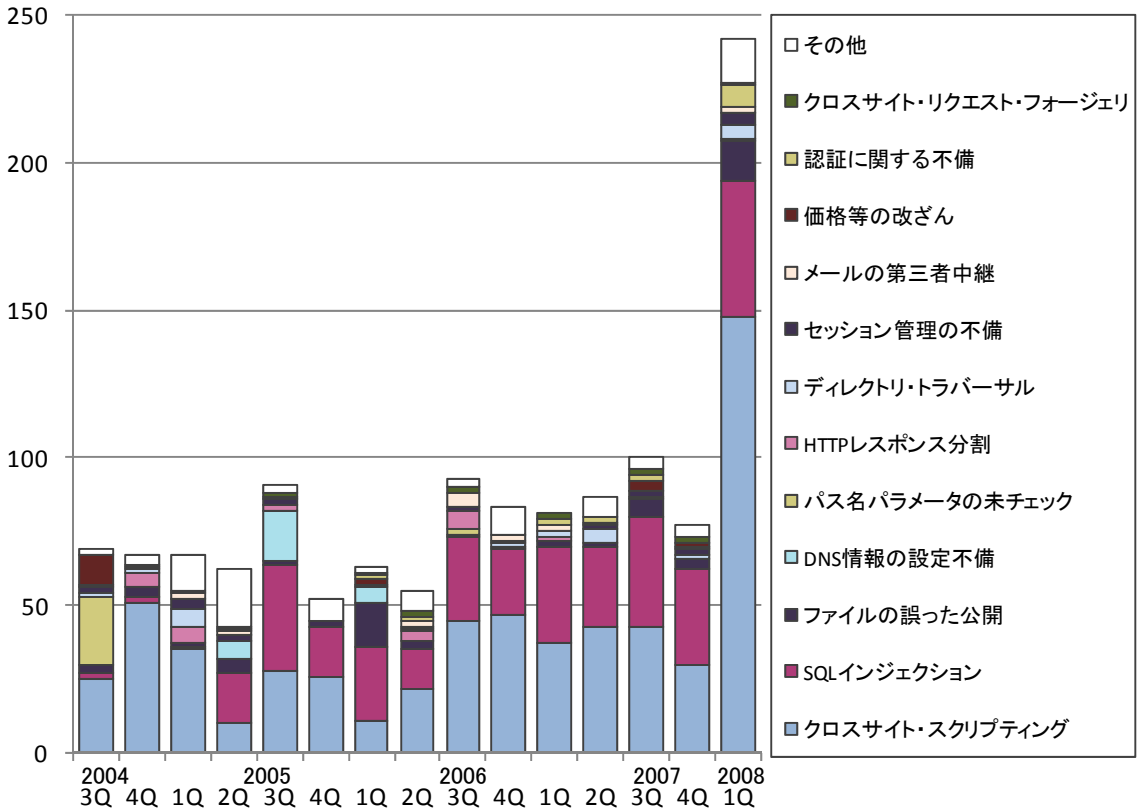
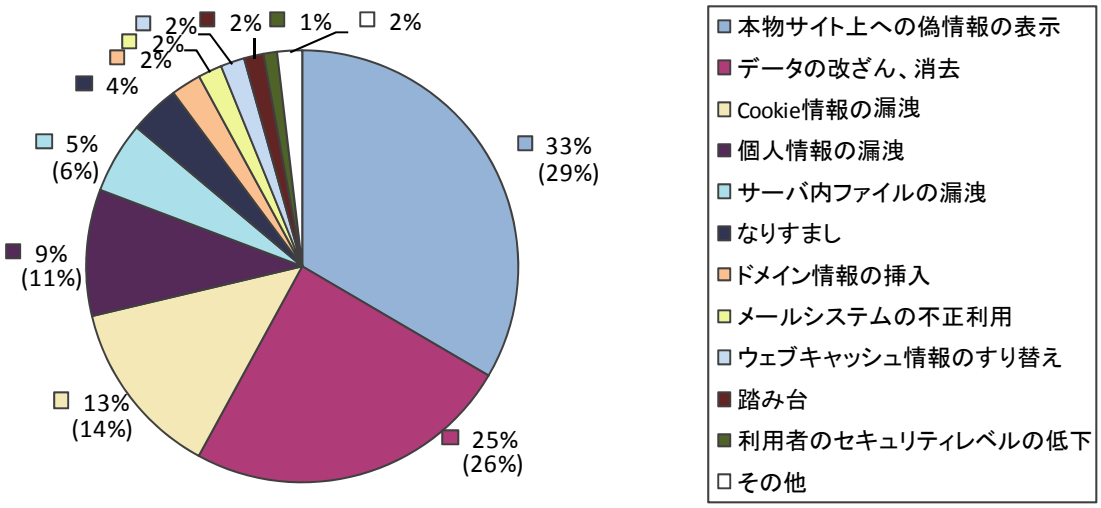


図2-3.ウェブサイトの脆弱性 種類別件数の推移（届出受付開始から2008年3月末まで）

[16] 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。



（1289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3月末まで）

今四半期も「クロスサイト・スクリプティング」が多く届出られ（図 2-3）、脆弱性の種類は「クロスサイト・スクリプティング」「SQL インジェクション」が全体の 7 割以上をしめます（図 2-2）。

また「クロスサイト・スクリプティング」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」「Cookie 情報の漏洩」「データの改ざん、消去」が約 7 割をしめています（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 3 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 53%の届出が 30 日以内、全体の 77%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

2007/2Q まで	2007/3Q まで	2007/4Q まで	2008/1Q まで
79%	79%	78%	77%

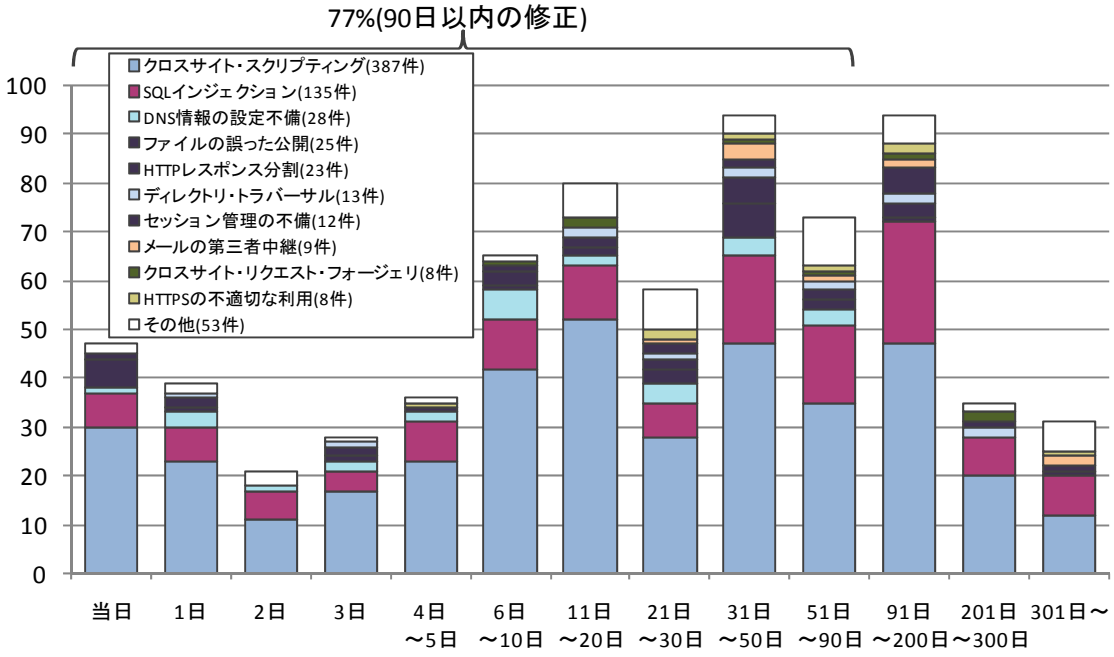


図2-5.ウェブサイトの修正に要した日数

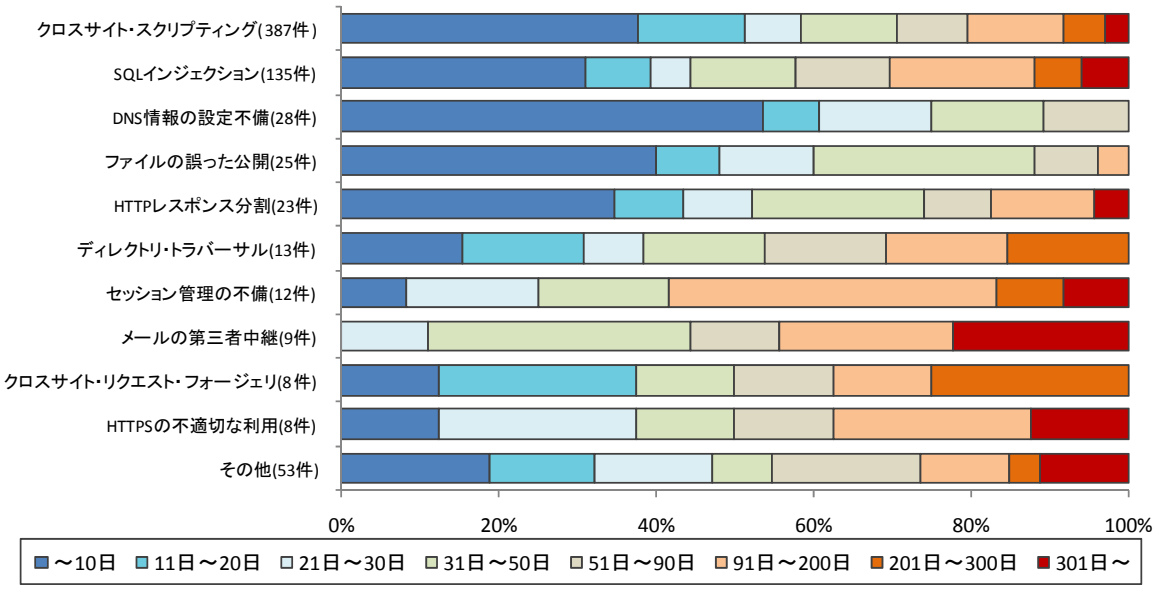


図2-6.ウェブサイトの修正に要した日数の傾向

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、セキュリティ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/

(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

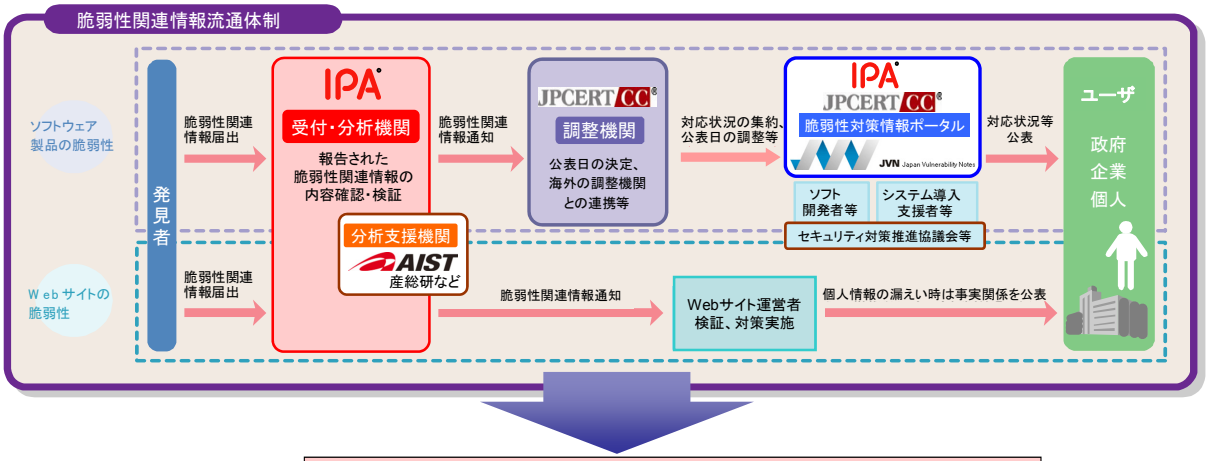
付表 2 ウェブサイト脆弱性の分類

	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