IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC®

プレスリリース
2007年7月19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 [2007年第2四半期(4月～6月)]

独立行政法人 情報処理推進機構(略称:IPA、理事長:藤原 武平太)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、2007 年第 2 四半期(4 月～6 月)の脆弱性関連情報の届出状況[1]をまとめました。

今四半期の呼びかけ:
「ソフトウェア製品開発者は、利用者に的確な脆弱性の対策情報を公表して下さい!」
—「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」[2]を参考に—

1. 2007 年第 2 四半期の届出状況

表 1 に示すように、2007 年 4 月 1 日から 6 月 30 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 **46** 件、ウェブアプリケーション(ウェブサイト)に関するもの **95** 件、合計 **141** 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 **501** 件、ウェブサイトに関するもの **940** 件、合計 **1,441** 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. 2007 年第 2 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	46 件	501 件
ウェブサイト	95 件	940 件
計	141 件	1441 件

(1)四半期毎の届出状況の推移

図1[3]に示すように、届出受付開始(2004 年 7 月 8 日)から各四半期末時点までの就業日 1 日あたりの届出件数が増加してきており、2007 年第 2 四半期末で **1.98** 件となりました。**近年、着実に増加しており、就業日 1 日あたり 2 件に近づいています。**

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	2005/2Q	2005/3Q	2005/4Q	2006/1Q	2006/2Q	2006/3Q	2006/4Q	2007/1Q	2007/2Q
1.45	1.43	1.58	1.59	1.61	1.70	1.75	1.92	1.95	1.98

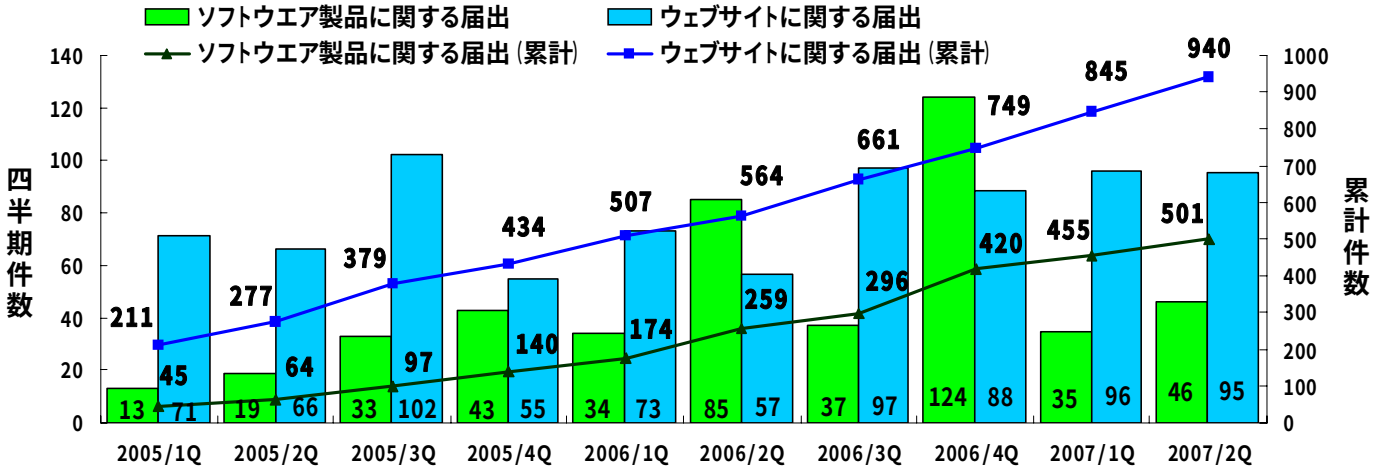


図1. 脆弱性関連情報の四半期別届出件数の推移

[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。

[2] 「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」を 2007 年 5 月より公開しました。
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

[3] 2007 年第 1 四半期に公表した四半期別届出件数の推移のグラフから、2007/1Q にウェブサイトとして届けられた 1 件を 2 つの問題として件数を追加するなどの変更をしました。

2.ソフトウェア製品の脆弱性の処理状況

表 2 に示すように、2007 年第 2 四半期にソフトウェア製品の脆弱性の修正が完了し JVN[4]で対策情報を公表したものは 23 件（届出受付開始からの累計 193 件）、製品開発者が脆弱性ではないと判断したものは 0 件（累計 29 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（累計 74 件）です。これらの取扱いを終了したものの合計は 26 件（累計 296 件）です。詳細は P.5 別紙 1 の1章を参照下さい。

表 2. ソフトウェア製品の脆弱性の処理件数

分類	件数	累計件数
公表済み	23 件	193 件
脆弱性ではない	0 件	29 件
不受理	3 件	74 件
計	26 件	296 件

(1)「Java Web Start」の脆弱性を注意喚起しました[5]

Java アプリケーションをウェブ経由でダウンロード及び実行するソフトである「Java Web Start」には、本来許可されていないシステムクラスが実行される脆弱性があり、悪意あるコードが利用者のコンピュータで実行される可能性がありました。

「Java Web Start」が同梱されている、JRE(Java Runtime Environment)は Java アプリケーションの実行環境として広く使われています。

この脆弱性対策を行うにあたり、使用中の JRE を異なるバージョンに更新した結果、一部の Java アプリケーションの動作に支障をきたす事例があったため、JRE を同一バージョンの update 版に更新する方法も合わせて、5 月 8 日に注意喚起しました。

(2)APOP 方式の脆弱性を注意喚起しました[6]

APOP（エーポップ、Authenticated Post Office Protocol）は、メールの受信に利用される認証方式の一つで、パスワードを盗聴から守るために使用されます。

APOP 方式には、プロトコル上の問題があり、利用者がなりすましたメールサーバに誘導された場合、メールの受信に利用するパスワードが解読され、漏えいする可能性がありました。

この APOP 方式の問題は MD5（エムディーファイブ、Message Digest 5）ハッシュ方式の問題がもととなっており、今回の問題が発見されたことは暗号学の国際会議で既に発表されているため、研究者の間で問題点の所在は周知のものとなっています。しかし、プロトコル上の問題であるため解決に時間がかかります。そのため、メールクライアントソフトの利用者への影響を考慮し、4 月 19 日に注意喚起しました。

(3)共通脆弱性評価システム CVSS[7]の新バージョンの概説資料を公開しました

共通脆弱性評価システム CVSS は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、米国家インフラストラクチャ諮問委員会（NIAC:National Infrastructure Advisory Council）のプロジェクトで 2004 年 10 月に原案が作成されました。

その後、CVSS の管理母体として CSIRT[8]の国際的な連合体である FIRST[9]が選ばれ、FIRST の CVSS-SIG(Special Interest Group)で適用推進や仕様改善が行われています。現在、CVSS は 30 を超える組織で採用されています[10]。

スペインで開催された FIRST 年会議で 6 月 20 日に CVSS の新バージョンである CVSS v2 が公表されたのに合わせ、その概説資料を公開しました。

CVSS 基本値の評価結果を公表している脆弱性対策情報データベース JVN iPedia や、脆弱性関連情報の調査結果[11]は、今後、CVSS v2 に順次対応していきます。

---

[4] Japan Vulnerability Notes。脆弱性対策情報ポータルサイト。国内製品開発者の脆弱性への対応状況を公開し、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] 本脆弱性の深刻度=レベルIII（危険）、CVSS 基本値=7.0、P.7 表 1-2 項番 1 を参照下さい。

[6] 本脆弱性の深刻度=レベルII（警告）、CVSS 基本値=4.0、P.7 表 1-2 項番 2 を参照下さい。

[7] Common Vulnerability Scoring System。http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

[8] Computer Security Incident Response Team。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。

[9] Forum of Incident Response and Security Teams。http://www.first.org/

[10] CVSS の採用組織：http://www.first.org/cvss/eadopters.html

[11] http://www.ipa.go.jp/security/vuln/documents/index.html

(4)望ましい脆弱性対策情報の公表マニュアルをまとめました

図 2 に JVN で公表した脆弱性対策情報の四半期別の公表件数を示します。届出受付開始から 2007 年第 2 四半期までに、国内発見者から IPA に届出があったもの累計 **193** 件の他に、海外の CSIRT から連絡を受けたもの累計 **261** 件を加え、合計 **454** 件の脆弱性対策情報を JVN で公表しました。

脆弱性対策情報を公表する際、ソフトウェア製品開発者は、利用者に的確な情報を提供することが望まれます。特に、既にリリースした製品に脆弱性が存在することを知りながら、脆弱性対策情報を公表せず、被害が生ずる可能性を隠したり、不十分な内容の公表にとどめたり、虚偽の内容を公表することは、利用者の情報資産や社会活動を危険にさらす結果を招きかねません。

このような状況から、利用者に必要な情報が的確に届けられることを目的に、**ソフトウェア製品開発者が行うべき脆弱性対策情報の望ましい公表手順について、具体的に公表すべき項目と公表例、脆弱性対策情報への誘導方法を記載した「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」を 5 月 30 日に公表しました。製品開発者は、本資料を参考にご対応くださいますようお願いします。**

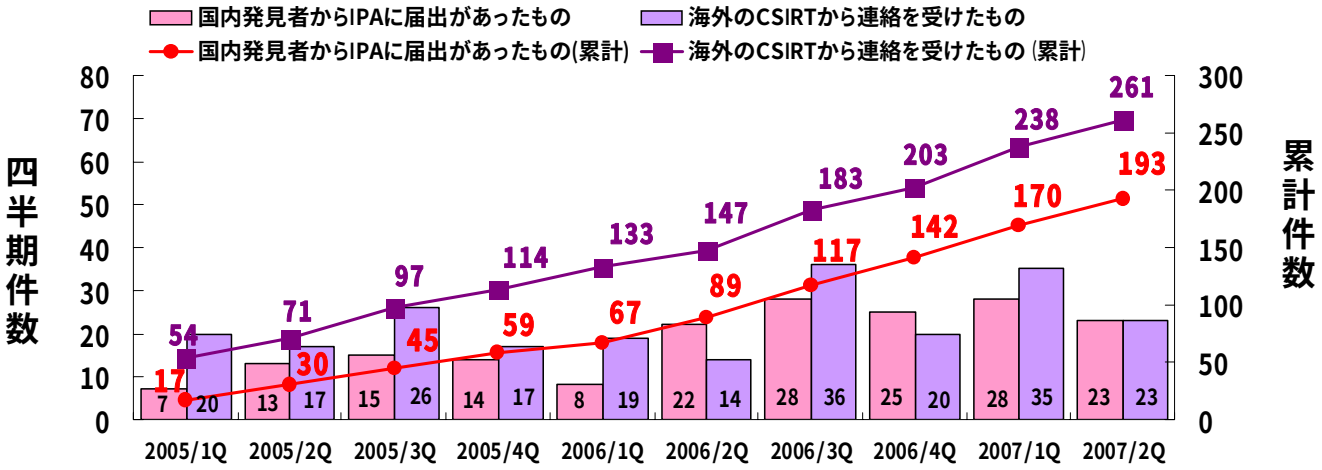


図2. JVNの脆弱性対策情報の四半期別公表件数の推移

(5) JVN のリニューアルを行い、見やすさの向上とコンテンツの充実を図りました

JVN の利用者や製品開発者からいただいたご意見に基づき、JVN の見やすさの向上とコンテンツの充実を図りました。また、**新たに、国内で利用されているソフトウェア等の製品を対象とした脆弱性対策情報データベース** JVN iPedia （ http://jvndb.jvn.jp/ ）**を 4 月 25 日に公開しました。**

JVN iPedia は、JVN で脆弱性対策情報を公表した約 450 件に加えて、海外の米国 NIST(National Institute of Standards and Technology)が運営する NVD(National Vulnerability Database)から日本向けの情報を収集･翻訳し、現在、約 3900 件の脆弱性対策情報を蓄積しています。また、目的の脆弱性対策情報を容易に探すための検索機能も用意しておりますので、ご活用下さい。

3.ウェブサイトの脆弱性の処理状況

表 3 に示すように、2007 **年第 2 四半期**にウェブサイトの脆弱性の修正が完了したものは **86** 件（届出受付開始からの累計 **629** 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（累計 **87** 件）、ウェブサイト運営者と連絡が不可能なものが**-6** 件[12]（累計 **7** 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 **7** 件（累計 **69** 件）です。これらの取扱いを終了したものの合計は **96** 件（累計 **792** 件）です。詳細は P.10 別紙 1 の 2 章を参照下さい。

表 3. ウェブサイトの脆弱性の処理件数

分類	件数	累計件数
修正完了	86 件	629 件
脆弱性ではない	9 件	87 件
連絡不可能	-6 件	7 件
不受理	7 件	69 件
計	96 件	792 件

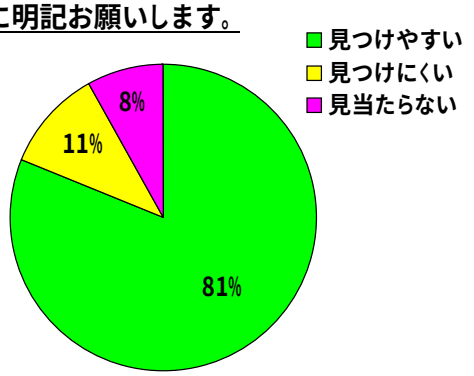
(1)ウェブサイトの連絡先窓口の明確化をお願いします

IPA では、ウェブサイトの脆弱性の届出を受付け、ウェブサイトの運営者に連絡を取り、届出の内容を伝え、脆弱性がある場合は対策をお願いしています。

[12] 当該ページが削除されたことを確認したものが 6 件あり、マイナス計上しました。

ウェブサイトへ連絡する際、連絡先窓口（メールアドレスや電話番号）をウェブサイトから探しだしますが、見つけにくい場合や見当たらない場合があります。2006 年 1 月から 2007 年 6 月末までの届出 506 件のうち、不受理 44 件を除いた 462 件のウェブサイトに連絡を取りましたが、約 2 割は連絡先窓口が見つけにくいか、もしくは見当たらないウェブサイトでした（図 3）。また、連絡先窓口に関して、ウェブサイトのうち約 3 割はウェブサイトが提供しているサービスに関する連絡先窓口でした（図 4）。サービスに関する連絡先窓口への脆弱性情報の連絡は、比較的、返信が無いことが多い傾向にあります。逆にウェブサイトに関する連絡先窓口がある場合は、返信が早い傾向があります。

ウェブサイト運営者は、ウェブサイトに問題が発生する事も想定し、ウェブサイトに対する連絡先窓口をウェブサイトに明記お願いします。



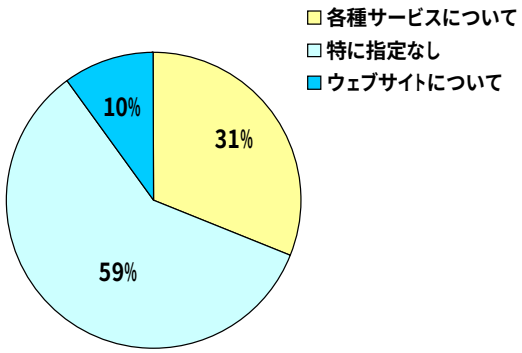


図3. ウェブサイト連絡先窓口のわかりやすさ　　**図4. ウェブサイト連絡先窓口の種類**

(2)ウェブサイトの問題を解決する体制の構築をお願いします

IPA では、ウェブサイトへ脆弱性情報を伝える場合、最初にウェブサイトの連絡先窓口へ対応者の確認（脆弱性の届出があったので返信を頂きたい旨の連絡）を行います。その後、脆弱性の詳細情報を伝えます。

最初の対応者の確認で連絡先窓口から返信が無い場合は、平均 5 営業日毎に再メールや電話などで連絡を試みます。2006 年 1 月から 2007 年 6 月末までの届出のうち修正が完了した 233 件について、1 回目の連絡で返信があった場合と、2 回以上の連絡が必要であった場合の、ウェブサイトへ脆弱性の詳細情報を伝えてから修正が完了するまでの修正日数の関係を図 5 に示します。

1 回の連絡で返信を頂けたウェブサイトの約 90%は 90 日以内に修正が完了しています。一方、2 回以上の連絡が必要だった場合は、90 日以内の修正が 80%になるなど、修正が長期化する傾向がやや見られます。

ウェブサイト運営者は、ウェブサイトに問題が発生する事を想定し、早期に問題に対応し、解決する体制の構築をお願いします。

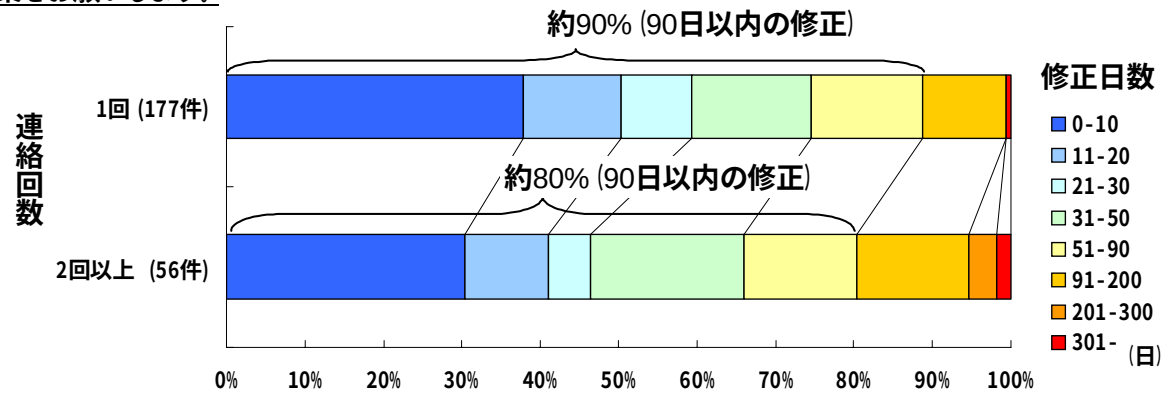


図5. IPAからウェブサイトへの連絡回数と修正日数の関係

■ 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
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**
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／佐々木
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

1. ソフトウェア製品の脆弱性関連情報の取扱いおよび調整

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、**23** 件（累計 **193** 件）です。また、「不受理」としたものは **3** 件（累計 **74** 件）です。

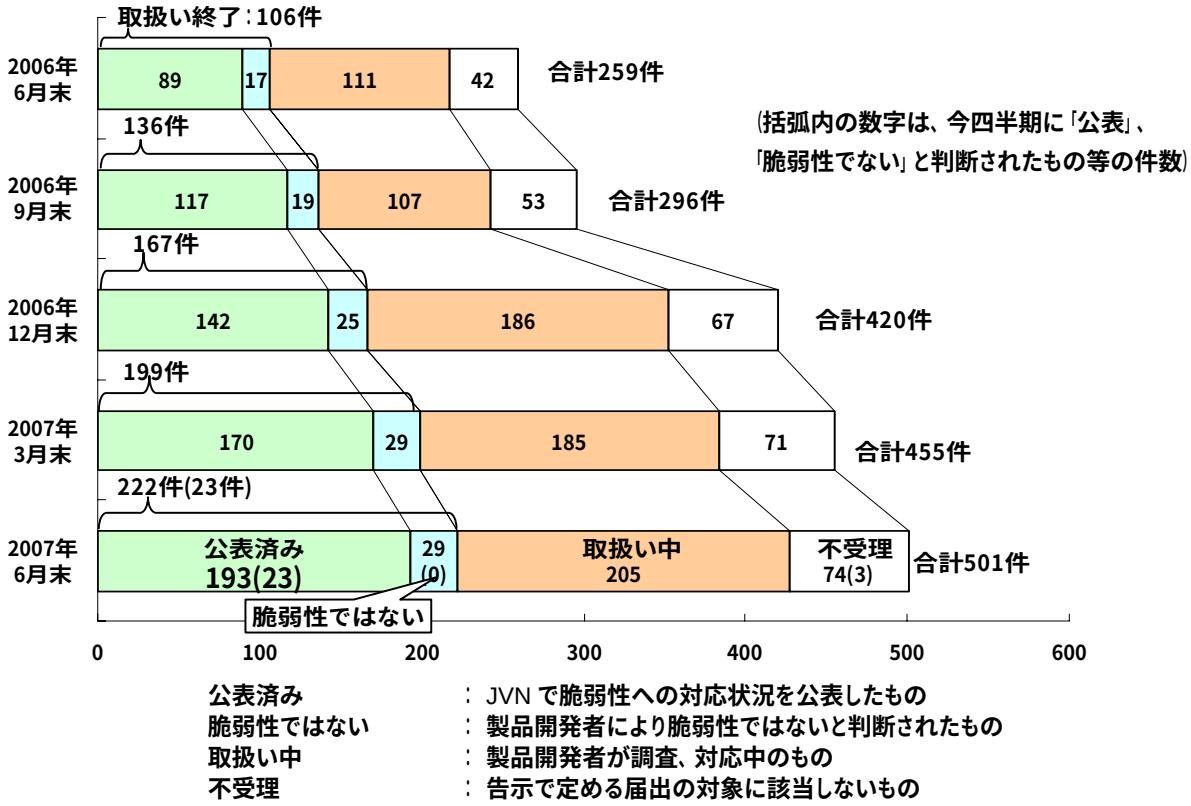
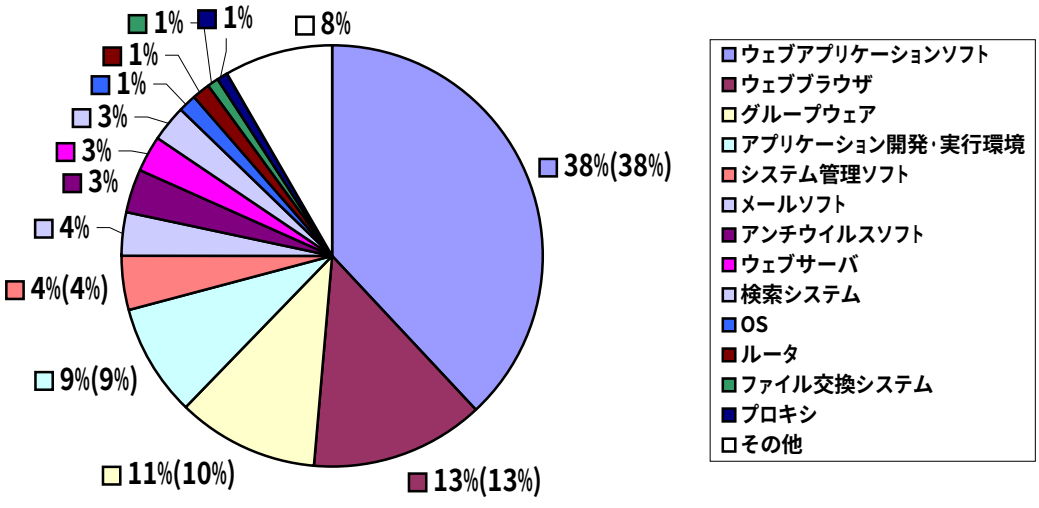


図 1-1. ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

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 **501** 件のうち、不受理のものを除いた **427** 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。



（427 件の内訳、グラフの括弧内は前四半期の数字）

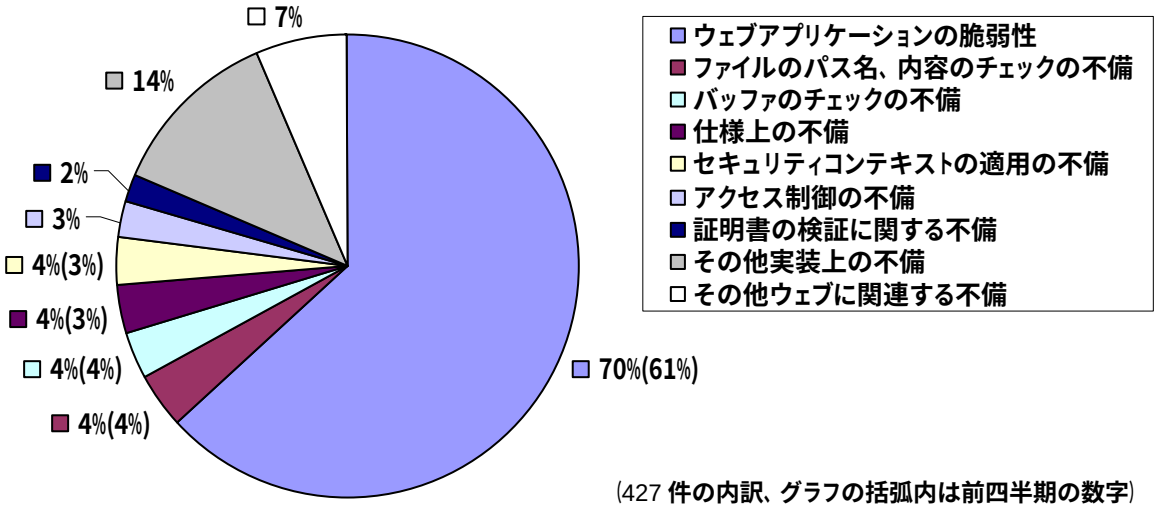
※　その他には、携帯機器、情報家電、パソコンの周辺機器、データベース、ワープロソフト等があります。

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 2007 年 6 月末まで）

1.3 脆弱性の原因と脅威

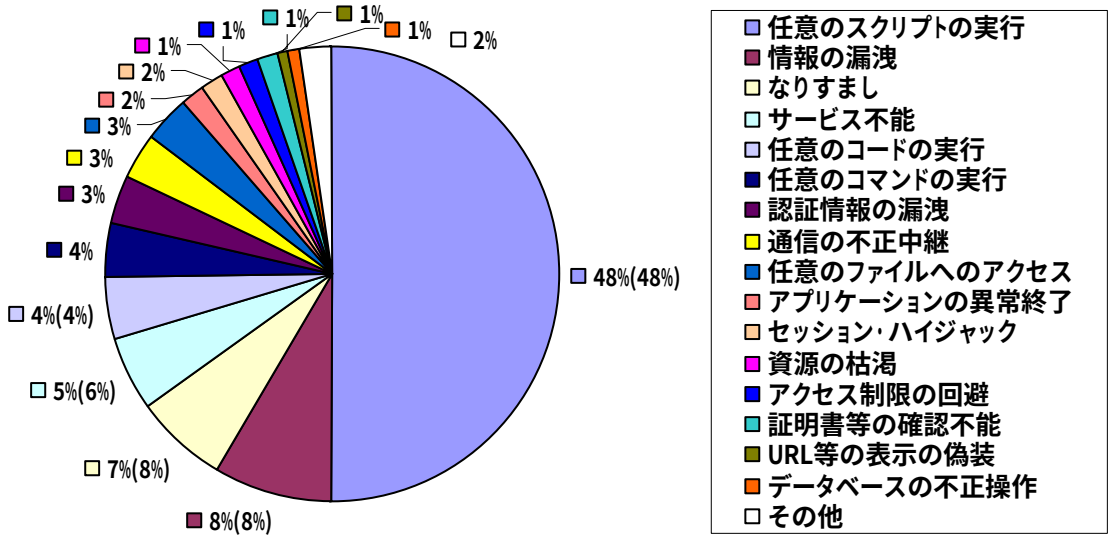
届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 **501** 件のうち、不受理のものを除いた **427** 件の原因別の内訳を図 1-3 に、脅威別の内訳を図 1-4 に示します。

図 1-3 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 1-4 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す。



(427 件の内訳、グラフの括弧内は前四半期の数字)

図 1-3.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 6 月末まで）[13]



(427 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 脅威別内訳（届出受付開始から 2007 年 6 月末まで）[1]

[13] 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。

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[14]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	23	193
②	海外 CSIRT 等と連携して公表したもの	23	261
	計	46	454

(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 2007 年 6 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 1-5 に示します。45 日以内に公表される件数が 36%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。

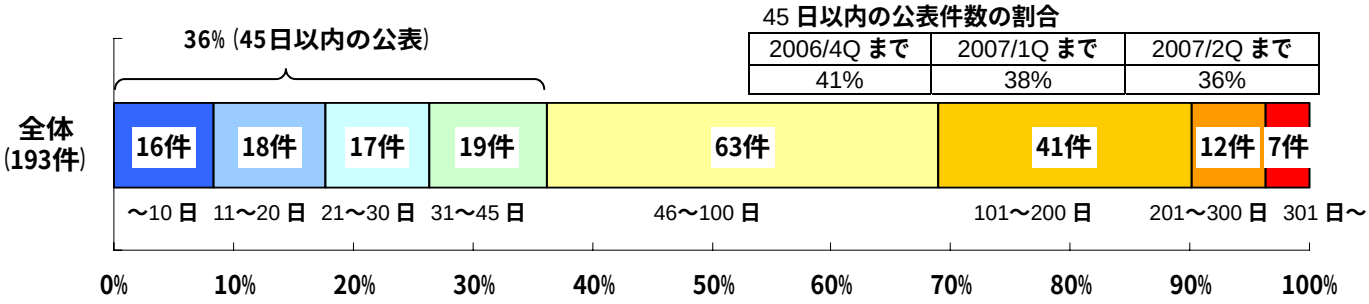


図 1-5.ソフトウェア製品の脆弱性 公表日数

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 10 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 1 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) ありました。

表 1-2.2007 年第 2 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	「Java Web Start」において許可されていないシステムクラスが実行される脆弱性	Java アプリケーションをウェブを通じてダウンロード及び実行するソフトである「Java Web Start」には、本来許可されていないシステムクラスが実行される脆弱性があります。このため、第三者により任意のコードが実行される可能性があります。	2007 年 5 月 8 日	7.0
脆弱性の深刻度=レベル II (警告)、CVSS 基本値=4.0～6.9				
2 (*3)	APOP におけるパスワード漏えいの脆弱性	メール受信プロトコルである「APOP」には、プロトコル仕様上の問題があります。このため、メールの受信に利用するパスワードが第三者により解読され漏えいする可能性があります。	2007 年 4 月 19 日	4.0
3	「ホームページ・ビルダー」付属の CGI サンプルプログラムにおける OS コマンド・インジェクションの脆弱性	ウェブページ作成ソフトである「ホームページ・ビルダー」付属の CGI サンプルプログラムには、利用者からの入力の処理に問題があります。このため、第三者によりサーバ上で任意の OS コマンドを実行される可能性があります。	2007 年 5 月 16 日	5.6

[14] 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。

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 I（注意）、CVSS 基本値=0.0～3.9				
4 (*1)	「私本管理 Plus Ver2 GOOUT」におけるディレクトリ・トラバーサルの脆弱性	個人用蔵書管理ソフト「私本管理 Plus」のデータ閲覧ソフトである「私本管理 PlusVer2 GOOUT」には、ディレクトリ・トラバーサルの問題があります。このため、第三者によりサーバ内の任意のファイルを閲覧される可能性があります。	2007 年 4 月 16 日	2.3
5 (*1)	「open-gorotto」におけるクロスサイト・スクリプティングの脆弱性	コミュニティサイト構築ソフトである「open-gorotto」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 4 月 16 日	1.9
6 (*2)	「InfoBarrier4」の自己復号型ファイルにおける脆弱性	情報漏洩防止セキュリティソフトである「InfoBarrier4」には、暗号機能で自己復号型ファイルとして作成したファイルに問題があります。このため、第三者により自己復号型ファイルの内容を閲覧されたり、自己復号パスワードを入手されたりする可能性があります。	2007 年 4 月 17 日	3.7
7	「キヤノン ネットワークカメラサーバー VB100 シリーズ」におけるクロスサイト・スクリプティングの脆弱性	ネットワークカメラサーバである「キヤノン ネットワークカメラサーバー VB100 シリーズ」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す。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 4 月 19 日	2.3
8	「Lunascape」の RSS リーダ機能において任意のスクリプトが実行される脆弱性	ウェブブラウザである「Lunascape」の RSS リーダ機能には、RSS 情報を HTML ページとして出力する際のエスケープ処理に漏れがあります。このため、意図しないスクリプトが実行される可能性があります。	2007 年 4 月 25 日	2.3
9	「Advance-Flow」におけるクロスサイト・スクリプティングの脆弱性	電子承認システム構築ソフトである「Advance-Flow」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 5 月 18 日	2.3
10 (*1)	「Mozilla Firefox」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザである「Mozilla Firefox」には、ウェブページの HTML を解釈する処理に問題があります。このため、意図しないスクリプトを実行する可能性があります。	2007 年 6 月 1 日	2.3
11	「HP System Management Homepage」におけるクロスサイト・スクリプティングの脆弱性	HP サーバ用システム管理ツールである「HP System Management Homepage」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 1 日	2.3
12 (*1)	「Meneame」におけるクロスサイト・スクリプティングの脆弱性	ソーシャルブックマークシステム構築ソフトである「Meneame」には、ウェブページを出力する際のｴｽｹｰﾌﾟ処理に漏れがあります。このため、第三者によりｳｪﾌﾞﾍﾟｰｼﾞにｽｸﾘﾌﾟﾄを埋め込まれる可能性があります。	2007 年 6 月 4 日	2.3
13	「ADPLAN」におけるクロスサイト・スクリプティングの脆弱性	ウェブアクセス測定システムである「ADPLAN」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 7 日	2.3
14 (*1)	「dotProject」におけるクロスサイト・スクリプティングの脆弱性	プロジェクト管理ツールである「dotProject」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 14 日	2.3
15 (*1)	「Apache Tomcat」におけるクロスサイト・スクリプティングの脆弱性	Java アプリケーションをサーバ側で動作させるソフトである「Apache Tomcat」の Web Application Manager には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 15 日	1.9
16 (*1)	「Apache Tomcat」付属のサンプルプログラムにおけるクロスサイト・スクリプティングの脆弱性	Java アプリケーションをサーバ側で動作させるソフトである「Apache Tomcat」付属のサンプルプログラムである jsp-examples には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりｳｪﾌﾞﾍﾟｰｼﾞにｽｸﾘﾌﾟを埋め込まれる可能性があります。	2007 年 6 月 15 日	2.3
17	「Internet Explorer」における MHTML 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	ウェブブラウザである「Internet Explorer」には、MHTML でウェブページにアクセスする際の処理に問題があります。このため、第三者によりウェブページで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す。	2007 年 6 月 18 日	1.9
18	「Internet Explorer」における MHTML により任意のスクリプトが実行される脆弱性	ウェブブラウザである「Internet Explorer」には、MHTML でウェブページにアクセスする際の処理に漏れがあります。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てしまう可能性があります。	2007 年 6 月 18 日	1.9
19 (*1)	「Apache Tomcat」の Accept-Language ヘッダの処理に関するクロスサイト・スクリプティングの脆弱性	Java アプリケーションをサーバ側で動作させるソフトである「Apache Tomcat」には、Accept-Language ヘッダに関する処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 19 日	2.3

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
20	「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	ウェブサーバである「雷電 HTTPD」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 21 日	2.3
21 (*1)	「Hiki」において任意のファイルが削除可能な脆弱性	Wiki クローンである「Hiki」には、セッション管理の処理に問題があります。このため第三者によりサーバ上のファイルを削除される可能性があります。	2007 年 6 月 25 日	1.9
22	「sHTTPd」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバである「sHTTPd」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 27 日	2.3
23 (*1)	「rktSNS」におけるクロスサイト・スクリプティングの脆弱性	コミュニティサイト構築ソフトである「rktSNS」には、ウェブページを出力する際のエスケープ処理に漏れがあります。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性があります。	2007 年 6 月 27 日	2.3

(*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

⑵ 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 23 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 TechnicalCyber Security Alert（表 1-4）の 11 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[15]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	MIT Kerberos 5 GSS-API ライブラリにおけるメモリ二重開放の脆弱性	複数製品開発者へ通知
2	MIT Kerberos 5 telnet deamon における任意のユーザとしてログインできる脆弱性	複数製品開発者へ通知
3	MIT Kerberos 5 krb5_klog_syslog() におけるスタックオーバーフローの脆弱性	複数製品開発者へ通知
4	BIND 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
5	Samba におけるコマンドインジェクションの脆弱性	注意喚起として掲載
6	Samba NDR MS-RPC 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
7	libpng 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	RSA BSAFE Cert-C および Crypto-C にサービス運用妨害 (DoS) の脆弱性	複数製品開発者へ通知
9	IPv6 Type0 ルーティングヘッダの問題	複数製品開発者へ通知
10	Yahoo! Messenger の Yahoo! Webcam view utilities ActiveX コントロールにバッファオーバーフローの脆弱性	特定製品開発者へ通知
11	Yahoo! Messenger の Yahoo! Webcam image upload ActiveX コントロールにバッファオーバーフローの脆弱性	特定製品開発者へ通知
12	JRE (Java Runtime Environment) のイメージ解析コード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

表 1-4.米国 US-CERT[16]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	MIT Kerberos に複数の脆弱性	複数製品開発者へ通知
2	Microsoft 製品における複数の脆弱性	緊急案件として掲載
3	Mozilla 製品における複数の脆弱性	緊急案件として掲載
4	Microsoft 製品における複数の脆弱性	緊急案件として掲載
5	Apple の Mac 製品に複数の脆弱性	緊急案件として掲載
6	Oracle 製品に複数の脆弱性	緊急案件として掲載
7	Microsoft DNS の RPC management インターフェース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
8	Microsoft 製品における複数の脆弱性	緊急案件として掲載
9	MIT Kerberos に複数の脆弱性	複数製品開発者へ通知
10	Microsoft Windows アニメーションカーソルの脆弱性	緊急案件として掲載
11	Microsoft Windows アニメーションカーソルにおけるスタックバッファオーバフローの脆弱性	緊急案件として掲載

[15] CERT/Coordination Center。1988 年のウィ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。
[16] United States Computer Emergency Readiness Team。米国の政府系 CSIRT。

2. ウェブサイトの脆弱性関連情報の取扱い

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 **89** 件（累計 **723** 件）でした。このうち、「修正完了」したものは **86** 件（累計 **629** 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 **87** 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」なもののうち **6** 件の当該ページが削除されているのを確認しましたので、累計 **7** 件としました。

取扱いを終了した累計 **723** 件のうち、「連絡不可能」を除く累計 **716** 件（**99%**）は、指摘され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確認されています。

「修正完了」したもの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 **9** 件（累計 **111** 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 **11** 件（累計 **61** 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 **18** 件）でした。

このほか、「不受理」としたものは **7** 件（累計 **69** 件）でした

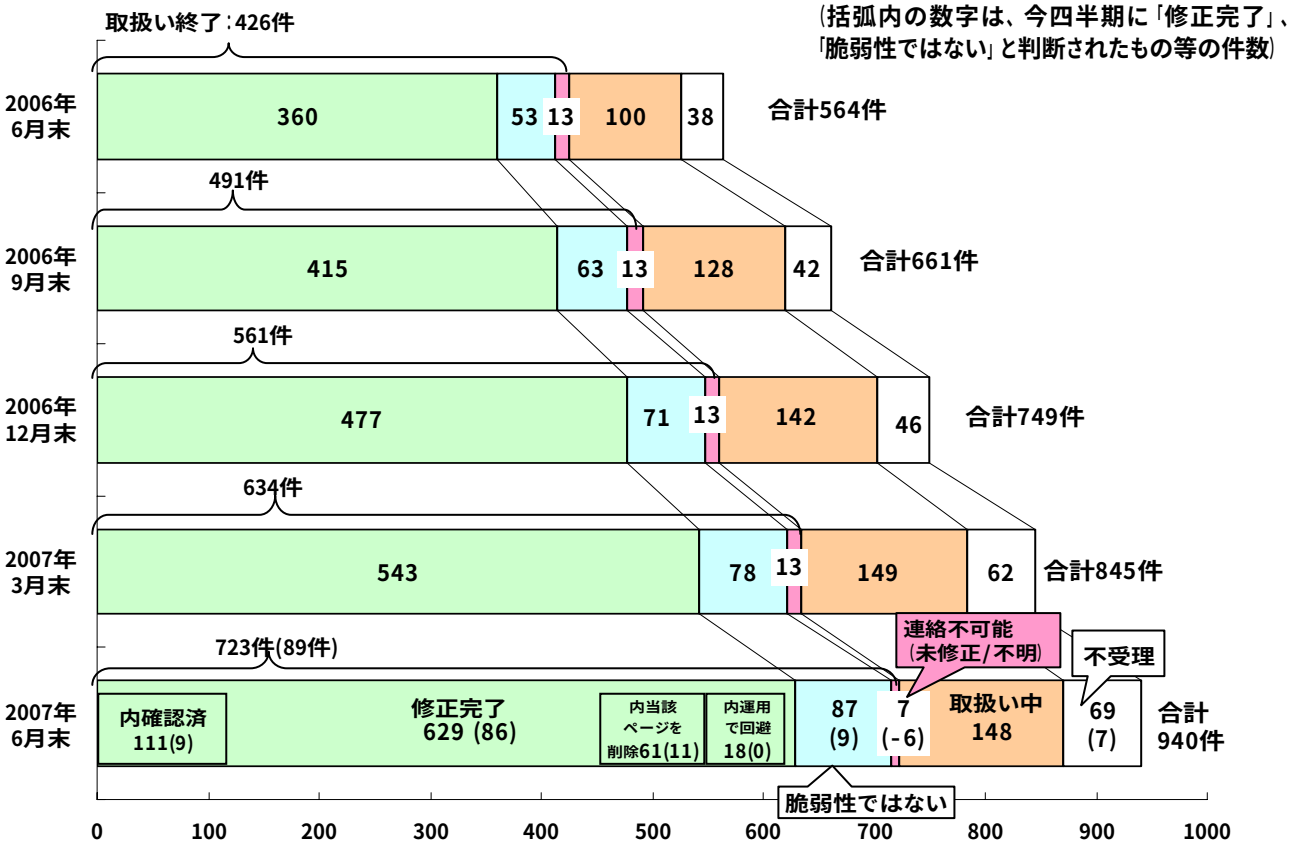
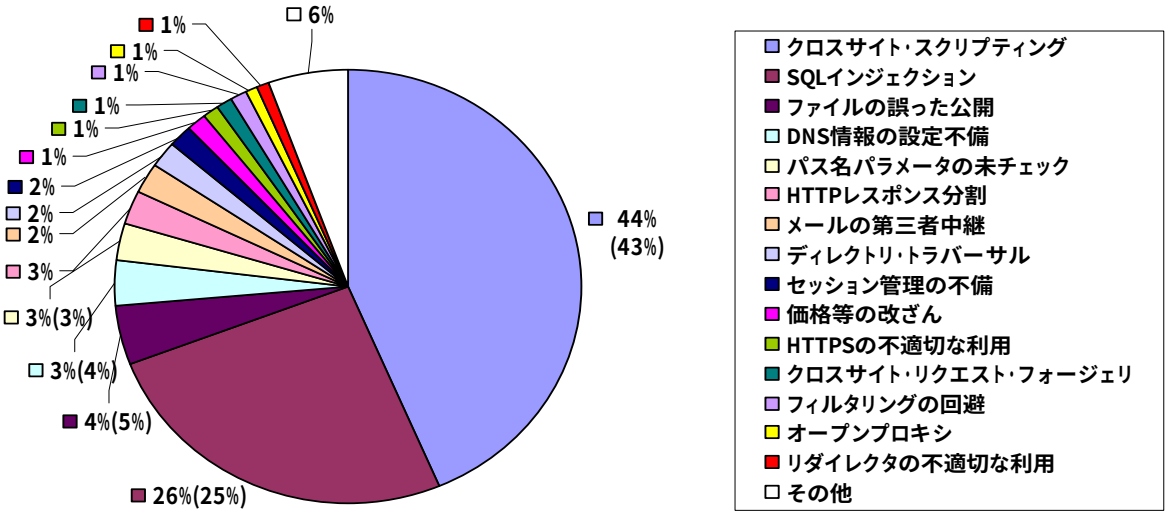


図 2-1. ウェブサイト各時点における脆弱性関連情報の届出の処理状況

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
取扱い中	：	ウェブサイト運営者が調査、対応中のもの
不受理	：	告示で定める届出の対象に該当しないもの

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**940**件のうち、不受理のものを除いた**871**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。



(871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2007年6月末まで）[17]

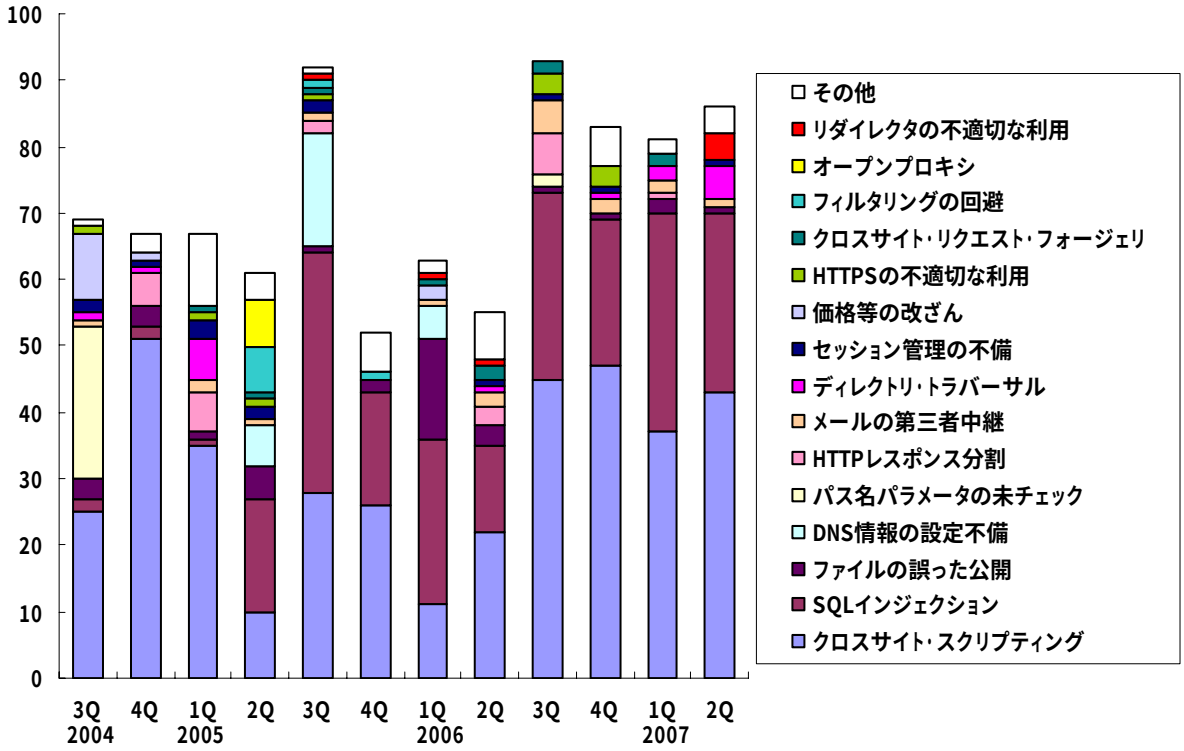
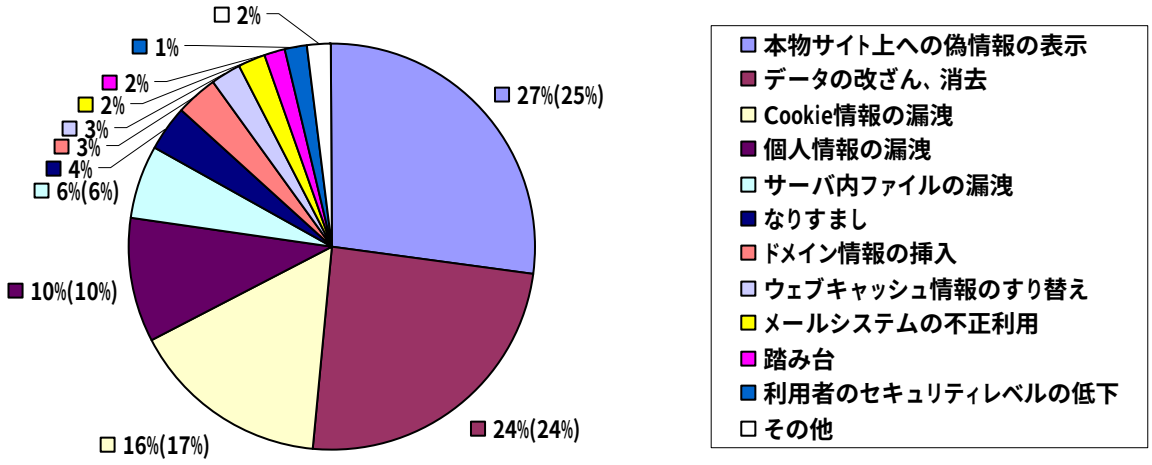


図2-3.ウェブサイトの脆弱性種類別件数の推移（届出受付開始から2007年6月末まで）[3]

[17] それぞれの脆弱性の詳しい説明については付表2参照してください。



(871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 2007 年 6 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 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 2007 年 3 月末までの届出について、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 79%の届出が 90 日以内に修正されています。

90 日以内の修正件数の割合

2006/4Q まで	2007/1Q まで	2007/2Q まで
80%	81%	79%

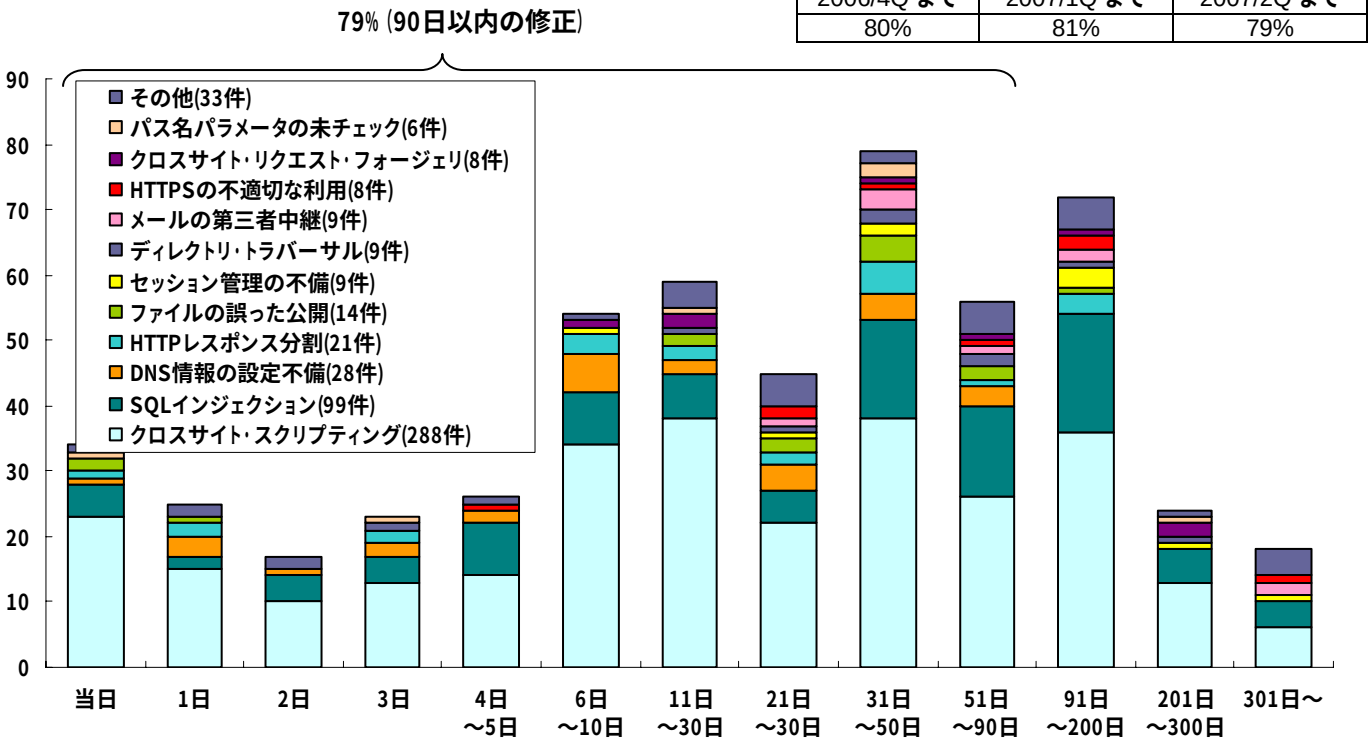


図 2-5.ウェブサイトの脆弱性修正に要した日数

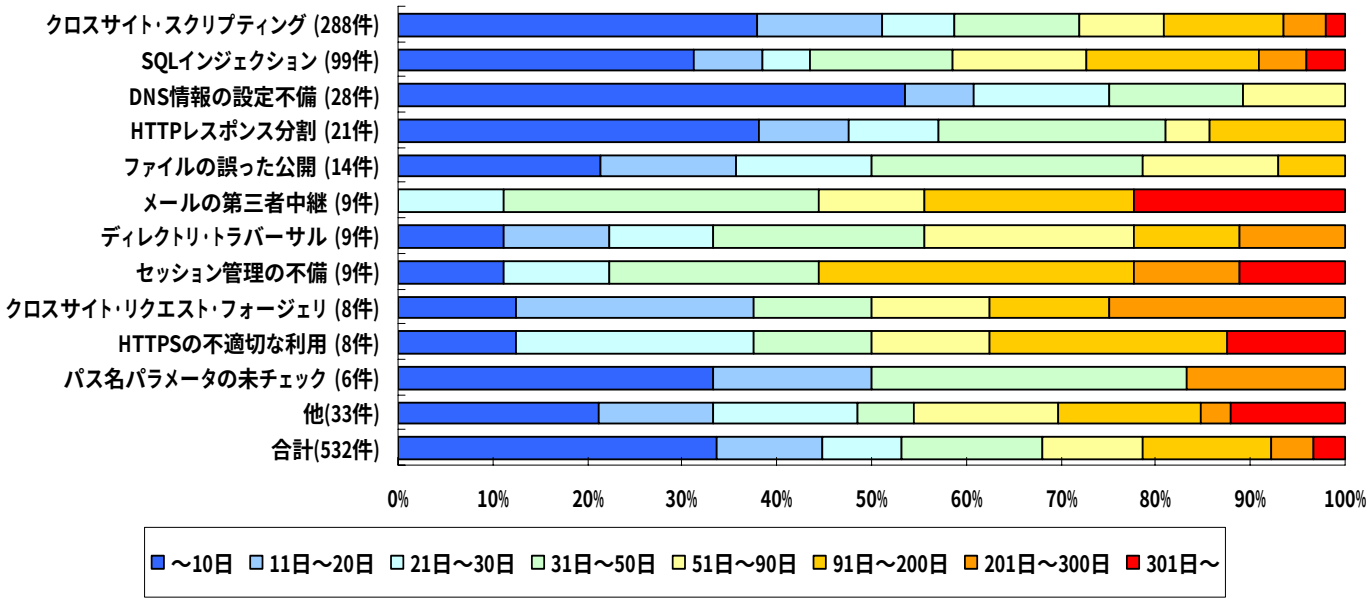


図 2-6.ウェブサイトの脆弱性修正に要した日数の傾向

3. 皆様へのお願い

脆弱性の修正を促進していくため、以下のとおり、ご注意ください。

(1)ウェブサイト運営者の皆様へ

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してください。

なお、脆弱性の理解にあたっては、以下のコンテンツをご利用ください。

「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)製品開発者の皆様へ

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報について、整備している「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」への登録にご協力ください（URL：http://www.jpcert.or.jp/vh/）。また、製品開発者ご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。IPA もしくは JPCERT/CC にご連絡下さい。

(3)一般インターネットユーザの皆様へ

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ください。脆弱性があるソフトウェアを使い続けることは避けましょう。

なお、脆弱性関連情報の適切な流通のために、発見者の皆様へも以下のとおりお願いします。

(4)発見者の皆様へ

届出いただきました脆弱性関連情報は、脆弱性が修正されるまでの間は第三者に漏れぬよう適切に管理くださるようお願いします。

参考

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

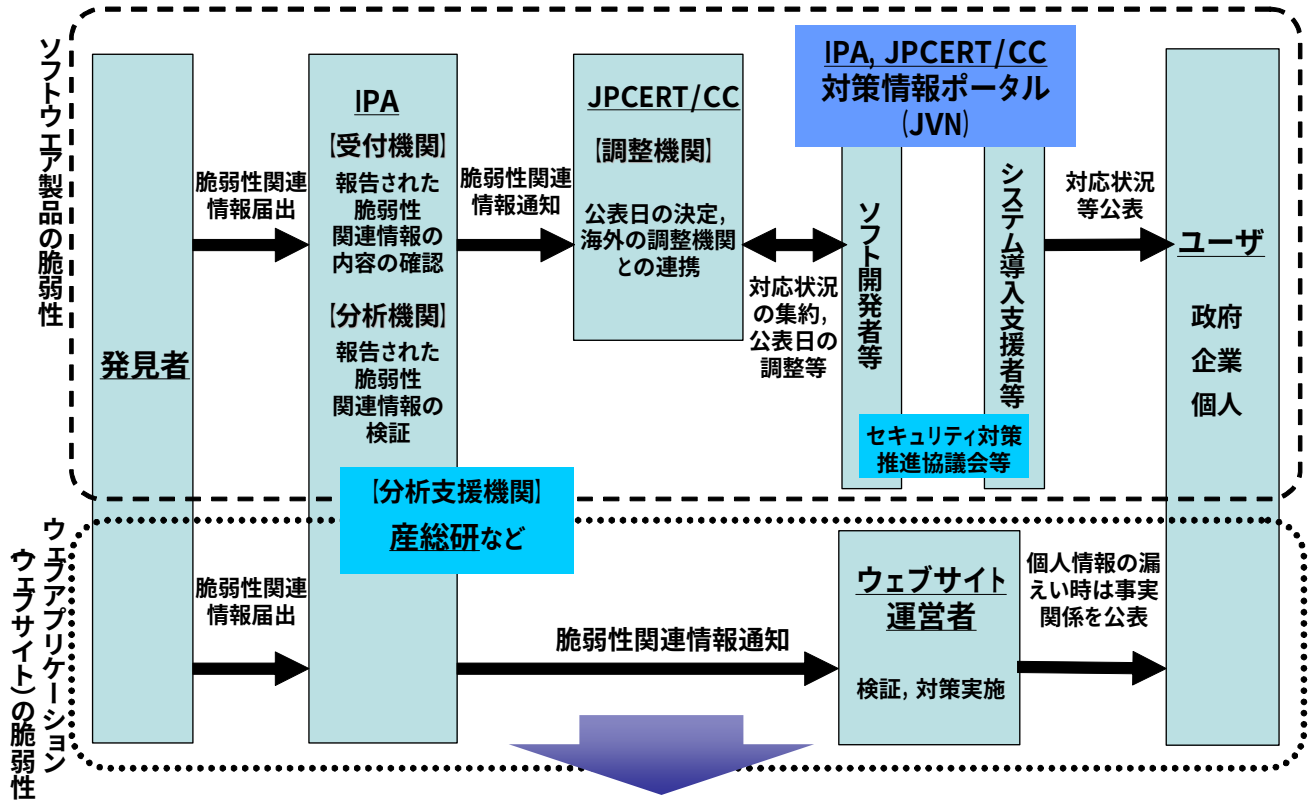
	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩

	脆弱性の種類	深刻度	説明	届出において想定された脅威
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
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

	脆弱性の種類	深刻度	説明	届出において想定された脅威
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、　・DNS : Domain Name System、
・CGI : Common Gateway Interface、　・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