プレスリリース

2007年 4 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 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: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 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。

今四半期の呼びかけ:

「ウェブサイトやソフトウェア製品の企画・設計段階から情報セキュリティを考慮した品質を作り込みましょう!」

—「安全なウェブサイトの作り方」「セキュア・プログラミング講座」「C/C++セキュアコーディング」(*2)などを参考に—

1. 2007 年第 1 四半期の届出状況

表 1 に示すように、2007 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 **36** 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 **131** 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 **455** 件、ウェブサイトに関するもの **844** 件、合計 **1,299** 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 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	届出	**36** 件	**455** 件
	脆弱性公表	**28** 件	**170** 件
ウェブアプリケーション(ウェブサイト)	届出	**95** 件	**844** 件
	修正完了	**53** 件	**456** 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 1 四半期末で **1.95** 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
1.45	1.43	1.58	1.59	1.61	1.70	1.75	1.92	1.95

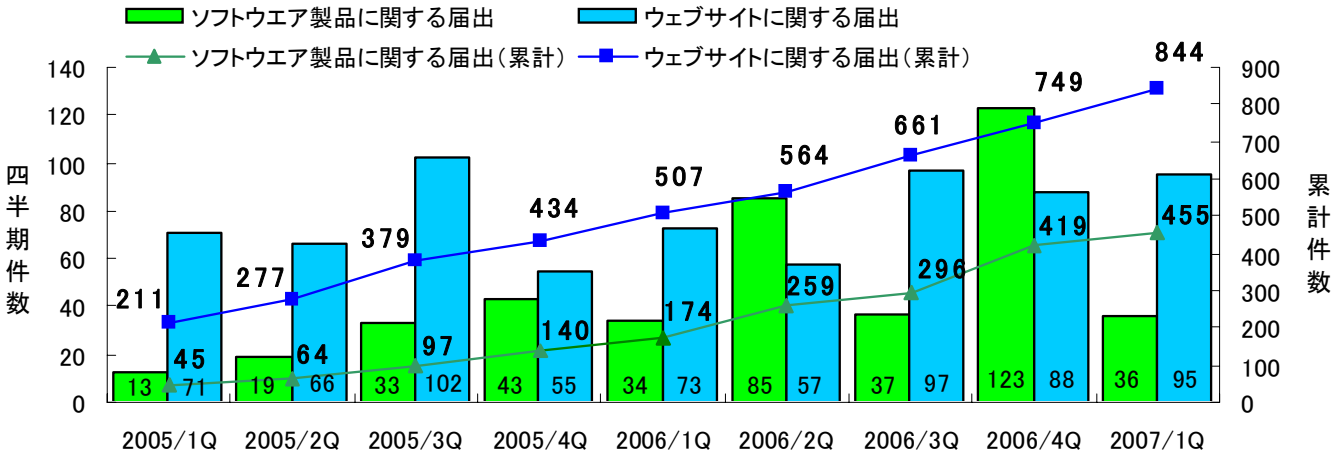


図1.脆弱性関連情報の四半期別届出件数の推移

2.ソフトウェア製品の脆弱性

(1)2007 年第 1 四半期から脆弱性の深刻度評価(*4)を開始しました

2007 年 2 月 22 日から、FIRST(*5)の場で適用推進などが行われている共通脆弱性評価システム CVSS(*6)を用い、ソフトウェア製品の脆弱性の深刻度評価を開始しました(*7)。

CVSS は、脆弱性そのものの特性を評価する「基本評価基準(Base Metrics)」、攻撃コードの出現有無や対策情報の利用可否などの現状の深刻度を評価する「現状評価基準（Temporal Metrics)」、製品利用者が対象製品の使用状況や攻撃を受けた場合の二次的な被害の大きさから最終的に深刻度を評価する「環境評価基準（Environmental Metrics）」から構成されます。

(2)脆弱性の深刻度評価には CVSS 基本値を用いています

IPA では、ソフトウェア製品の脆弱性の深刻度評価は、CVSS の「基本評価基準(Base Metrics)」を用い、CVSS 基本値(Base Score)を算出し、脆弱性そのものの特性について深刻度評価を行っています。

表 2 に示すように、CVSS 基本値は、脆弱性に対する攻撃がインターネット経由で可能か否か、攻撃に必要な条件の複雑さはどうか、攻撃前に認証(Authentication）が必要か否か、などの項目を評価して算出します。また、情報システムに求められるセキュリティ特性、「機密性（Confidentiality Impact）」、「完全性(Integrity Impact）」、「可用性(Availability Impact）」の3つの要素に対する影響度も加味して算出します。

CVSS 基本値は、機密性・完全性・可用性の3つの要素に同時に影響を与えるものほど高くなります。

表2.CVSS基本値の評価基準

(1)攻撃元区分	ローカル		リモート(*a)
(2)攻撃条件の複雑さ	高		低
(3)攻撃前の認証(*b)要否	必要		不要
(4)機密性への影響（情報漏えいの可能性）	なし	部分的	全面的
(5)完全性への影響（情報改ざんの可能性）	なし	部分的	全面的
(6)可用性への影響（業務停止の可能性）	なし	部分的	全面的

(*a)：インターネット経由で攻撃可能、(*b)：Authentication

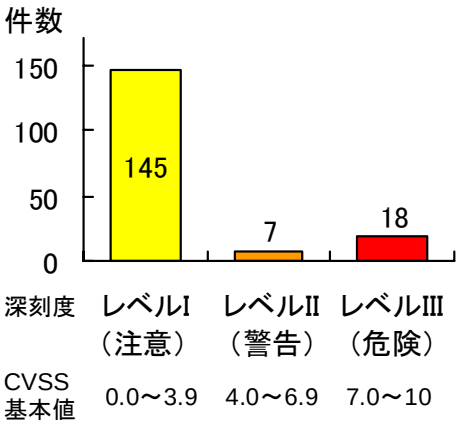


図2.公表済み脆弱性の深刻度分布

(3)2007 年第 1 四半期末までに公表した脆弱性の深刻度

届出受付開始から 2007 年第 1 四半期末までに JVN(*8)で脆弱性対策情報を公表した 170 件のソフトウェア製品の脆弱性の深刻度は図 2 にのようになっています。レベル III（危険）が 18 件、レベルII（警告）が 7 件、レベル I（注意）が 145 件ありました。レベル III（危険）やレベル II（警告）に分類される深刻度の高いものには、OS コマンドインジェクション、SQL インジェクション、バッファオーバーフローなどの脆弱性がありました。

(4)2007 年第 1 四半期に公表した脆弱性の概要

2007 年第 1 四半期に JVN で公表した 28 件のソフトウェア製品の脆弱性の中に、深刻度が高いレベル III（危険）が 1 件、レベルII（警告）が 2 件ありました（P.7 表 1-2 項番 1,2,3）。レベルII（警告）の 2 件は、RSS(*9)情報を取り扱う製品です。RSS 関連はレベル I（注意）にも 2 件(表 1-2 項番 6,13)あり、計 4 件ありました。

RSS は、ウェブサイトの更新情報やニュース情報の配信などを利用者が効率的に把握できる技術として普及してきています。外部情報を定期的に取得する機能を持つソフトウェア製品は、情報セキュリティを考慮した品質の作り込みが特に重要です。

3.ウェブサイトの脆弱性

届出受付開始（2004 年 7 月 8 日）から 2007 年第 1 四半期末までに届出を受付た累計 844 件のうち、不受理 62 件を除いた 782 件のウェブサイトの運営主体は、企業合計が 70%、各種協会・社団法人などの団体が 9%、個人サイトが 8%などとなっています（図 3）。

また、届出対象のウェブサイト数で見ると、累計 578 サイトに対して届出があり、一つのウェブサイトに対して 1 件の届出があったものは 86%、同一ウェブサイトに 2 件～4 件の届出があったものが 12%、5 件～9 件が 1%、10 件以上が 1%ありました（図 4）。

同一ウェブサイトに対する複数の届出の中には、届出られたウェブページ以外のウェブページにも脆弱性があった事例がありました。また、一度、脆弱性を対策しても、ウェブサイトの更新や再構築などにより、新たな脆弱性を作り込んだ事例もありました。

ウェブサイト運営者は、一過性のセキュリティ対策ではなく、情報セキュリティマネジメントとして継続的にセキュリティ対策および運用を行い、セキュリティレベルを保つことが重要です。

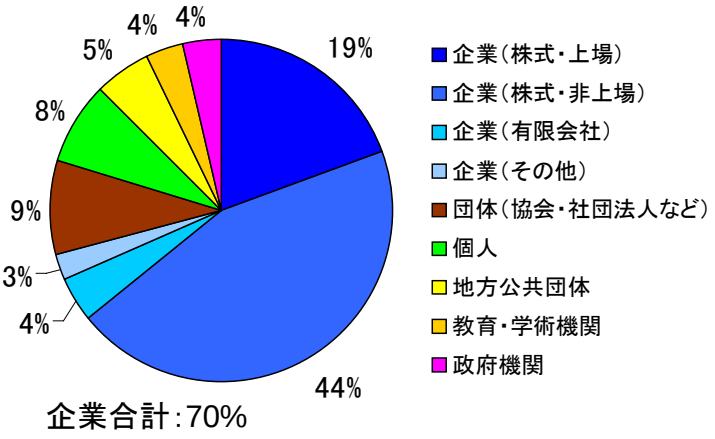


図3.ウェブサイトの運営主体

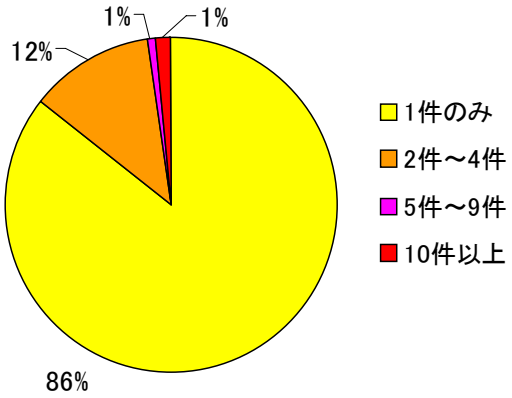


図4.各ウェブサイトの脆弱性件数

『脚注』

(*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)「安全なウェブサイトの作り方　改訂第 2 版」：http://www.ipa.go.jp/security/vuln/websecurity.html
「セキュア・プログラミング講座」：http://www.ipa.go.jp/security/awareness/vendor/programming/index.html
「C/C++　セキュアコーディング」：http://www.jpcert.or.jp/securecording_book.html

(*3)2006 年第 4 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、2006/4Q にウェブサイトに関して届出られた1件を、ソフトウェア製品に関する届出として変更するなどを変更しました。

(*4)脆弱性の深刻度評価：http://www.ipa.go.jp/security/vuln/SeverityLevel.html

(*5)FIRST：Forum of Incident Response and Security Teams。http://www.first.org/

(*6)CVSS：Common Vulnerability Scoring System。http://www.ipa.go.jp/security/vuln/SeverityCVSS.html

(*7)脆弱性関連情報の調査結果：http://www.ipa.go.jp/security/vuln/documents/index.html

(*8)JVN：脆弱性対策情報ポータルサイトです。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 および JPCERT/CC が共同で運営しています。http://jvn.jp/

(*9)RSS：RDF(Resource Description Framework) Site Summary。主にウェブサイトの更新情報を公開するのに使用されている構造化されたデータ形式。

■ 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

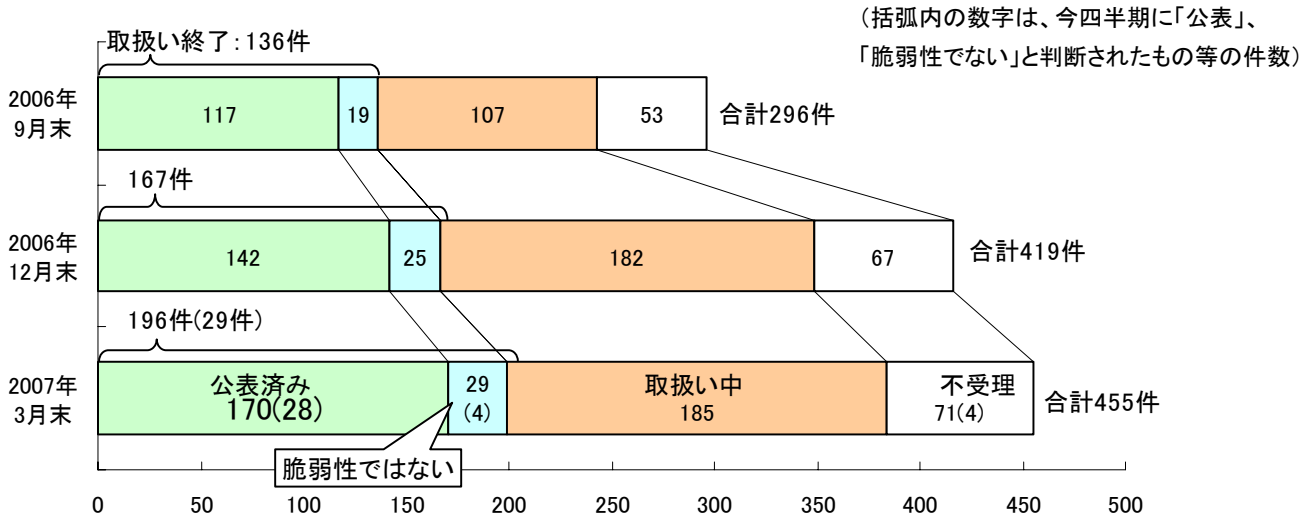
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503　Fax:03-5978-7510　E-mail: pr-inq@ipa.go.jp
有限責任中間法人 JPCERT コーディネーションセンター 経営企画室 広報 江田
Tel:03-3518-4600　Fax:03-3518-4602　E-mail: pr@jpcert.or.jp

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、**28** 件（累計 **170** 件）です。また、「不受理」としたものは **4** 件（累計 **71** 件）です。



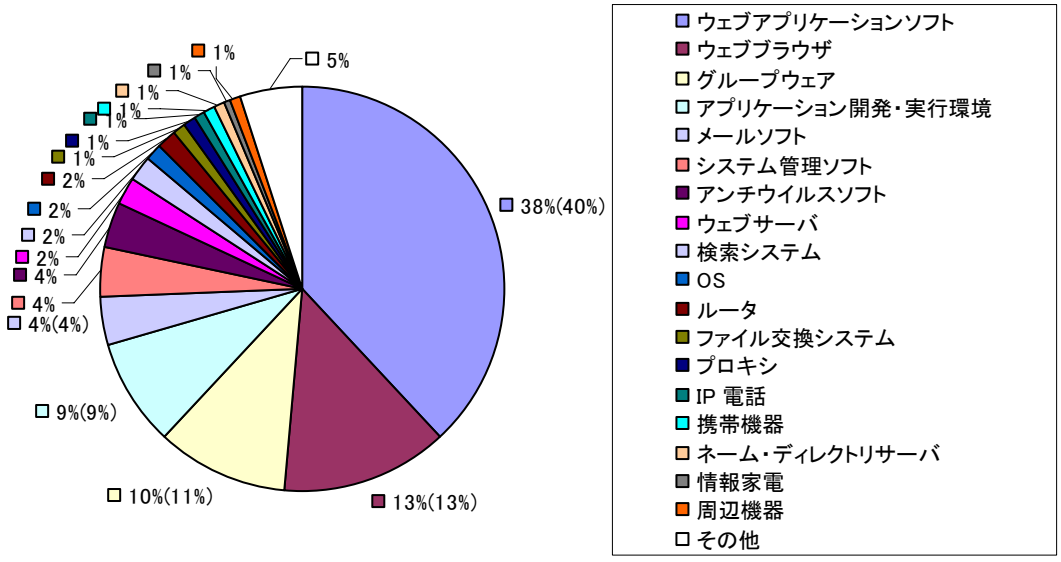
公表済み	：	JVN で脆弱性への対応状況を公表したもの
脆弱性ではない	：	製品開発者により脆弱性ではないと判断されたもの
取扱い中	：	製品開発者が調査、対応中のもの
不受理	：	告示で定める届出の対象に該当しないもの

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 **455** 件のうち、不受理のものを除いた **384** 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。また、パソコンなどのコンピュータ上で動くソフトウェアだけでなく、携帯機器や情報家電、パソコンの周辺機器などに関するものが含まれています。



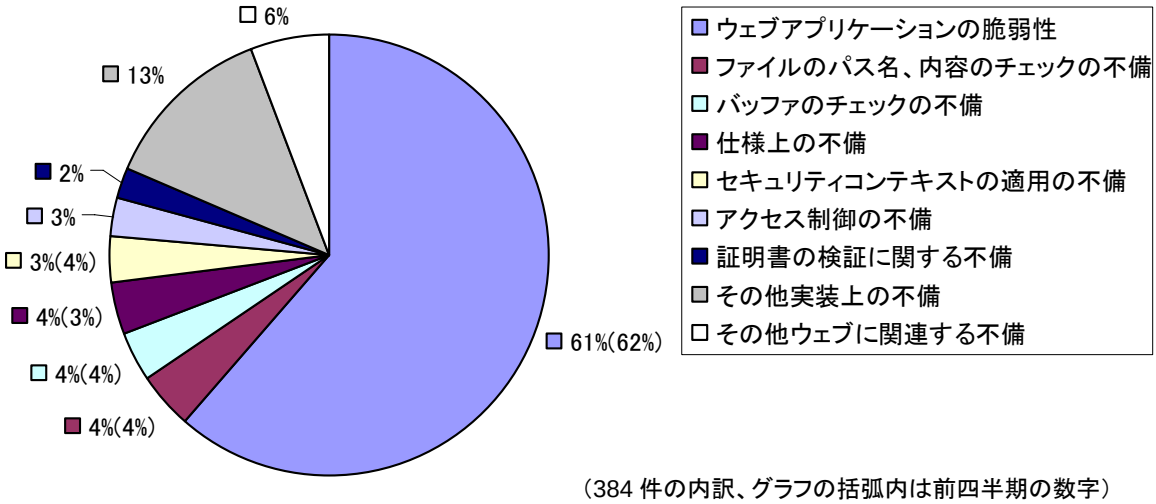
※　その他には、データベース、ワープロソフト等があります　　（384 件の内訳、グラフの括弧内は前四半期の数字）

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 3 月末まで）

1.3 脆弱性の原因と脅威

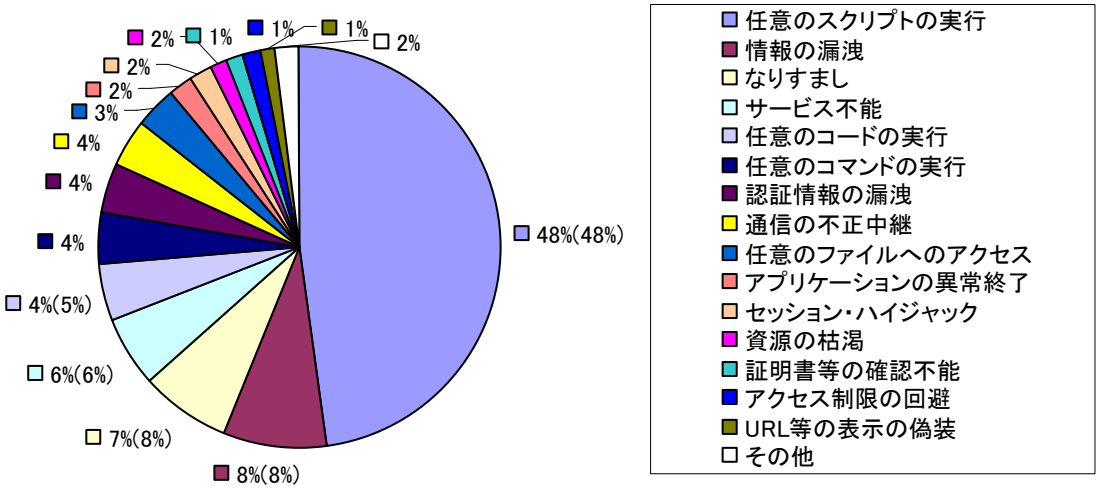
届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 **455** 件のうち、不受理のものを除いた **384** 件の原因別の内訳を図 1-3 に、脅威別の内訳を図 1-4 に示します。

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。



（384 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 3 月末まで）[1]



（384 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 3 月末まで）[1]

[1] 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、および海外 CSIRT[2]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 JP Vendor status Notes（JVN）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	28	170
②	海外 CSIRT から連絡を受けたもの	21	162
	計	49	332

(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 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 1-5 に示します。全体の 38%の届出が 45 日以内に公表されています。

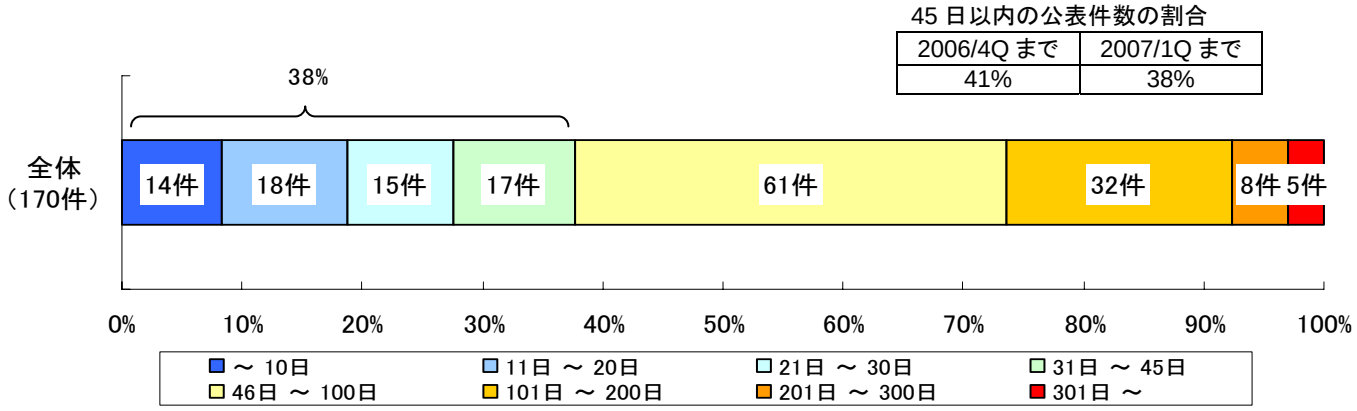


図 1-5. ソフトウェア製品の脆弱性 公表日数

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 8 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 3 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 2 件（表 1-2 の*3）ありました。

今四半期は RSS 情報を取り扱うソフトウェア製品の脆弱性対策情報を公表しました（表 1-2 の項番 2, 3, 6, 13）。RSS は、ウェブサイトの更新情報やニュース情報の配信など、頻繁に情報が更新されるウェブサイトで利用されており、複数のウェブサイトの更新情報を利用者が効率的に把握できる技術として普及してきています。今回の公表は、不特定多数の人が書き込める情報に意図しないスクリプトが埋め込まれてしまう脆弱性の一つとして、対策情報を公表したものです。外部情報を定期的に取得する機能を持つソフトウェア製品は、情報セキュリティを考慮した品質の作り込みが特に重要です。

[2] 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。

表 1-2. 2007 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）				
1 (*1) (*2)	「ショッピングバスケットプロ」における OS コマンドインジェクションの脆弱性	ショッピングサイト構築ソフトである「ショッピングバスケットプロ v7」には、入力内容の検査処理が適正に行われない OS コマンドインジェクションの脆弱性が存在します。このため、第三者によりウェブサーバで任意のコマンドを実行される可能性があります。	2007 年 1 月 25 日	7.0
脆弱性の深刻度=レベル II（警告）				
2 (*1)	「Sage」において任意のスクリプトが実行される脆弱性	Mozilla Firefox に RSS 情報の管理機能を追加する機能拡張である「Sage」には、RSS 情報を HTML ページに変換する際の処理が不適切なため、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。スクリプトの内容によっては、コンピュータ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 2 月 9 日	4.7
3 (*3)	「NewsGlue」と「いきなり事情通」において任意のスクリプトが実行される脆弱性	RSS 情報を管理するソフト「NewsGlue」および「いきなり事情通」には、RSS 情報を HTML ページに変換する際の処理が不適切なため、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。スクリプトの内容によっては、コンピュータ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 3 月 22 日	4.7
脆弱性の深刻度=レベル I（注意）				
4	「Serene Bach」におけるクロスサイト・スクリプティングの脆弱性	ブログ作成ソフト「Serene Bach」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 1 月 5 日	2.3
5 (*1)	「Drupal」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「Drupal」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 1 月 17 日	2.3
6	「フレッシュリーダー」における RSS フィード クロスサイト・スクリプティングの脆弱性	RSS 情報を管理するソフト「フレッシュリーダー」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 1 月 18 日	2.3
7 (*1)	「phpAdsNew」におけるクロスサイト・スクリプティングの脆弱性	オープンソースのウェブ広告作成・管理システム「phpAdsNew」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 1 月 22 日	2.3
8	「Movable Type」におけるクロスサイト・スクリプティングの脆弱性	ウェブログを作成・管理するためのシステム「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 1 月 23 日	2.3
9	CGI RESCUE 製「WebFORM」におけるメール内容欠落の脆弱性	フォームメール「WebFORM」には、メールの本文部分へ挿入される入力値の処理が適切に行われない問題があります。このため、ウェブ管理者に届くメールから、メール送信者に関する情報が欠落する可能性があります。	2007 年 1 月 25 日	2.3
10	CGI RESCUE 製「WebFORM」におけるクロスサイト・スクリプティングの脆弱性	フォームメール「WebFORM」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 1 月 25 日	2.3
11	CGI RESCUE 製「WebFORM」における HTTP ヘッダインジェクションの脆弱性	フォームメール「WebFORM」には、HTTP ヘッダを出力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に偽の情報が表示される可能性があります。	2007 年 1 月 25 日	2.3
12 (*1)	「b2evolution」におけるクロスサイト・スクリプティングの脆弱性	ブログ作成ソフト「b2evolution」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 1 月 26 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
13	「Sleipnir」の RSS バーにおけるセキュリティゾーンの扱いに関する脆弱性	ウェブブラウザ「Sleipnir」の RSS バーには、RSS 情報がセキュリティ制限の緩いゾーンで取り扱われてしまう問題があります。このため、セキュリティ制限の緩いゾーンで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 1 月 26 日	1.9
14 (*1)	「MODx」におけるクロスサイト・スクリプティングの脆弱性	オープンソースの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 1 月 29 日	2.3
15 (*2)	「CCC クリーナー」におけるバッファオーバーフローの脆弱性	ボット駆除ツール「CCC クリーナー」には、バッファオーバーフローの脆弱性が存在します。このため、第三者により任意のコードを実行されたり、サービス不能状態になる可能性があります。	2007 年 2 月 10 日	3.9
16	「ColdFusion」におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーション開発支援のためのフレームワークである「ColdFusion」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 2 月 14 日	2.3
17	「ColdFusion」のエラー画面におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーション開発支援のためのフレームワークである「ColdFusion」のエラー画面には、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 2 月 14 日	2.3
18	「Adobe JRun」におけるクロスサイト・スクリプティングの脆弱性	J2EE（Java 2 Platform Enterprise Edition）に準拠したアプリケーションサーバである「Adobe JRun」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 2 月 14 日	2.3
19	「アリエル・エアワン・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	プロジェクトやスケジュールの管理ソフトである「アリエル・エアワン・シリーズ」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 2 月 16 日	2.3
20 (*2)	「CCC クリーナー」における UPX 圧縮実行ファイル検索処理にゼロ除算の脆弱性	ボット駆除ツール「CCC クリーナー」には、UPX 圧縮実行ファイルの検索処理においてゼロ除算の脆弱性が存在します。 このため、「CCC クリーナー」が異常終了したり、システムが異常終了する可能性があります。	2007 年 3 月 12 日	3.3
21 (*1)	「Trac」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「Trac」には、Internet Explorer を利用した場合、コンテンツに含まれるスクリプトが実行されてしまう問題があります。	2007 年 3 月 13 日	2.3
22	「FENCE-Pro」および「Systemwalker Desktop Encryption」の自己復号型ファイルにおける脆弱性	暗号化ソフトウエア「FENCE-Pro」および「Systemwalker Desktop Encryption」には、作成した自己復号型ファイルに問題があります。このため、正しいパスワードを知らなくとも復号できる可能性があります。	2007 年 3 月 16 日	3.7
23	「Interstage Application Server」におけるクロスサイト・スクリプティングの脆弱性	アプリケーションの実行・開発環境「Interstage Application 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 3 月 19 日	2.3
24	「BASP21」においてメールの不正送信が可能な脆弱性	Windows OS で動作する汎用コンポーネント「BASP21」には、管理者が設定していない宛先や内容で電子メールを送信してしまう問題があります。このため、第三者により任意の宛先へ不正にメールを送信される可能性があります。	2007 年 3 月 26 日	2.3
25 (*3)	「CruiseWorks」および「みんなでオフィス」におけるアクセス制限回避の脆弱性	グループウェア「CruiseWorks」および「みんなでオフィス」には、ユーザのアクセス制限が適切に行われていない問題があります。このため、一般ユーザがシステム設定や登録情報を変更できてしまう可能性があります。	2007 年 3 月 29 日	2.0
26 (*1)	「Overlay Weaver」におけるクロスサイト・スクリプティングの脆弱性	オーバレイネットワークの構築およびエミュレーション環境を提供するソフト「Overlay Weaver」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 3 月 30 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
27	「MailDwarf」においてメールの不正送信が可能な脆弱性	メールフォーム CGI「MailDwarf」には、管理者が設定していない宛先や内容で電子メールを送信してしまう問題があります。このため、第三者により任意の宛先へ不正にメールを送信される可能性があります。	2007 年 3 月 30 日	2.3
28	「MailDwarf」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 CGI「MailDwarf」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 3 月 30 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

(2)海外 CSIRT から連絡を受け公表した脆弱性

表 1-3 に海外 CSIRT から連絡を受けた脆弱性を示します。海外 CSIRT から連絡を受けた脆弱性情報は、登録された国内の製品開発者のうち関連する製品開発者へ通知したうえ、日本語訳を JVN に掲載しています。今四半期は、米国 CERT/CC(Computer Emergency Response Team/ Coordination Center)から**21** 件の脆弱性関連情報の連絡を受けました。このほか、**13** 件の US-CERT Technical Cyber Security Alert を JVN で公表しました。

表 1-3. CERT/CC から連絡を受け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 の Real Time Streaming Protocol (RTSP) 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	Kerberos administration daemon が適切に関数ポインタを初期化しない問題	複数製品開発者へ通知
3	Kerberos administration daemon が初期化されていないポインタを解放する問題	複数製品開発者へ通知
4	Cisco IOS が細工された IP オプションを含むパケットを適切に処理できない問題	特定製品開発者へ通知
5	Cisco IOS が不正な IPv6 パケットを適切に処理できない問題	特定製品開発者へ通知
6	Cisco IOS における TCP パケットを適切に処理できない問題	特定製品開発者へ通知
7	Microsoft Word 2000 に文字列処理に関する脆弱性	注意喚起として掲載
8	Cisco IOS における SIP パケットの処理に関する脆弱性	注意喚起として掲載
9	Microsoft Office 製品において任意のコードが実行される脆弱性	注意喚起として掲載
10	Trend Micro AntiVirus が細工された UPX 圧縮実行ファイルを適切に処理できない脆弱性	注意喚起として掲載
11	Microsoft Word に文字列を適切に処理できない脆弱性	注意喚起として掲載
12	ベリサインの 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	注意喚起として掲載
13	デバイスエクスプローラ HIDIC OPC サーバ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
14	デバイスエクスプローラ FA-M3 OPC サーバ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
15	デバイスエクスプローラ SYSMAC OPC サーバ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
16	デバイスエクスプローラ TOYOPUC OPC サーバ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
17	デバイスエクスプローラ MODBUS OPC サーバ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
18	デバイスエクスプローラ MELSEC OPC サーバ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
19	OpenBSD の IPv6 パケット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
20	NETxAutomation 社製 NETxEIB OPC Server に OPC server handle を適切に処理できない脆弱性	注意喚起として掲載
21	Microsoft Windows アニメーションカーソル ANI ヘッダにおけるスタックバッファオーバーフローの脆弱性	注意喚起として掲載

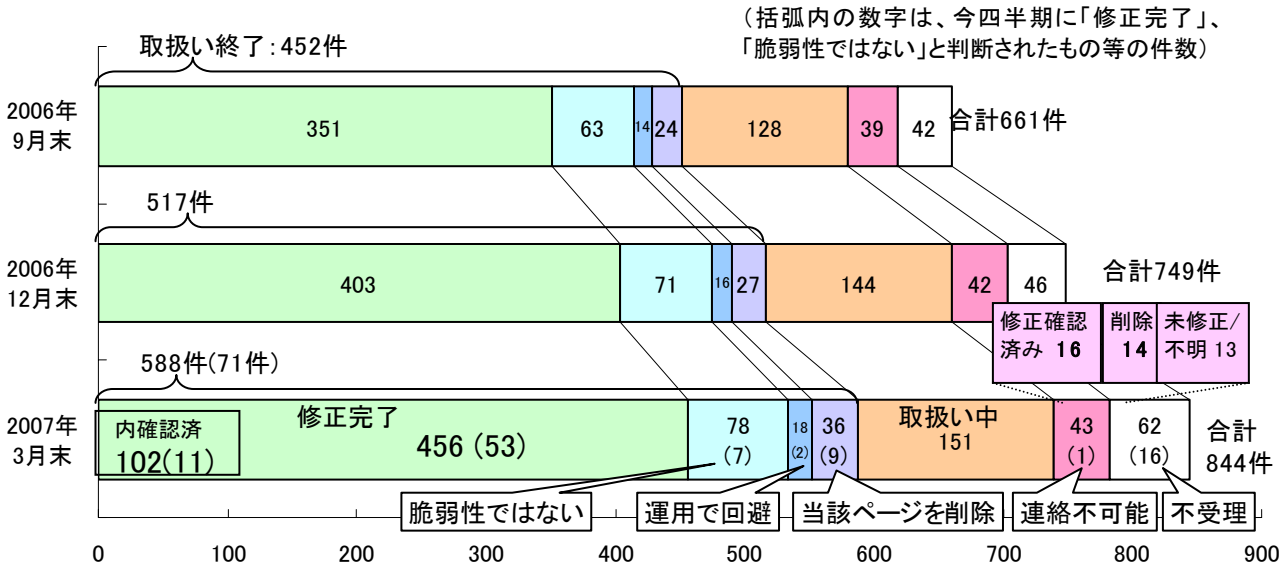
2. ウェブサイトの脆弱性関連情報の取扱い

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は、今四半期中に処理を終了したものは **71** 件（累計 **588** 件）でした。このうち、「修正完了」したものは **53** 件（累計 **456** 件）、ウェブサイト運営者により「脆弱性はない」と判断されたものは **7** 件（累計 **78** 件）ありました。「修正完了」したものうちの **11** 件（累計 **102** 件）は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 が確認しました。

このほか、「不受理」としたものが **16** 件（累計 **62** 件）ありました。「連絡不可能」の届出のうち、**16** 件は修正されています。その中には、ウェブサイト運営者からの回答がないためレンタルサーバ会社と連絡を取り修正が確認できたサイト、脆弱箇所の記述が削除されていることが確認できたサイトがあります。また、**14** 件は、当該ページ自体が削除されており、脆弱性がなくなっていることを確認しています。メールや電話でウェブサイト運営者と連絡が取れない場合は、郵送手段などでの連絡を試みています。

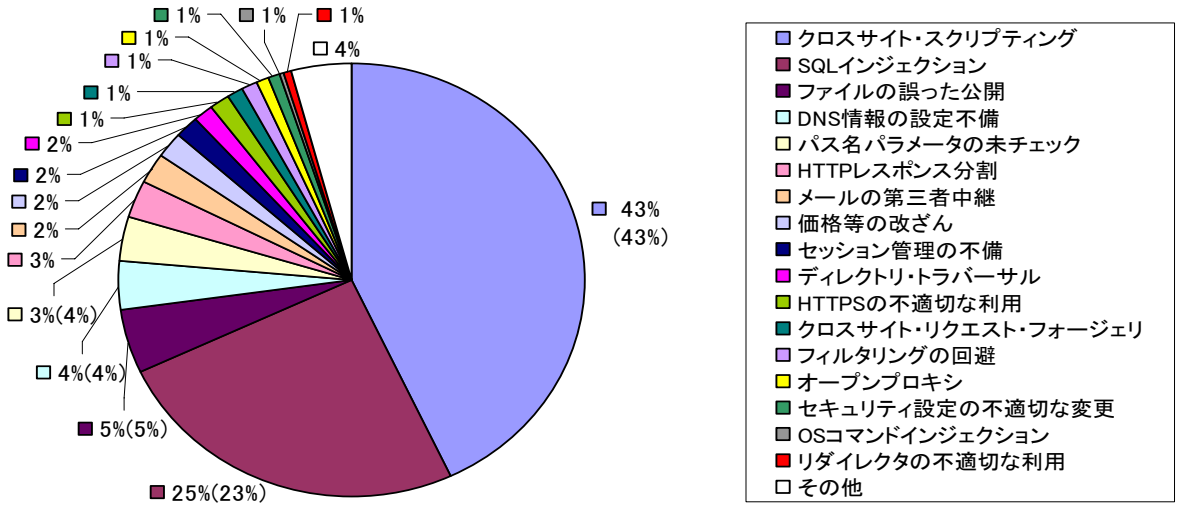


修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
脆弱性ではない	：	ウェブサイト運営者により脆弱性はないと判断されたもの
運用で回避	：	修正はせず、運用により被害を回避しているもの
当該ページを削除	：	修正ではなく当該ページを削除することで対応されたもの
確認済	：	修正完了のうち、IPA が修正を確認したもの
取扱い中	：	ウェブサイト運営者が調査、対応中のもの
連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
不受理	：	告示で定める届出の対象に該当しないもの

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 **844** 件のうち、不受理のものを除いた **782** 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。



（782 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 3 月末まで）[3]

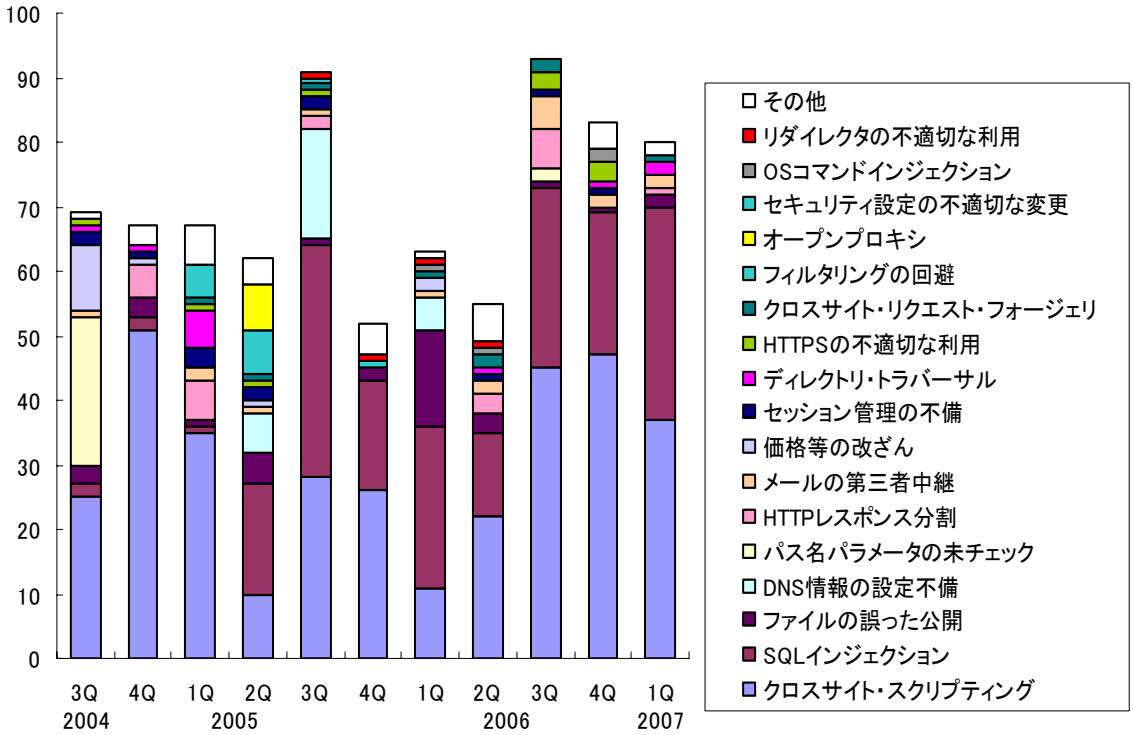
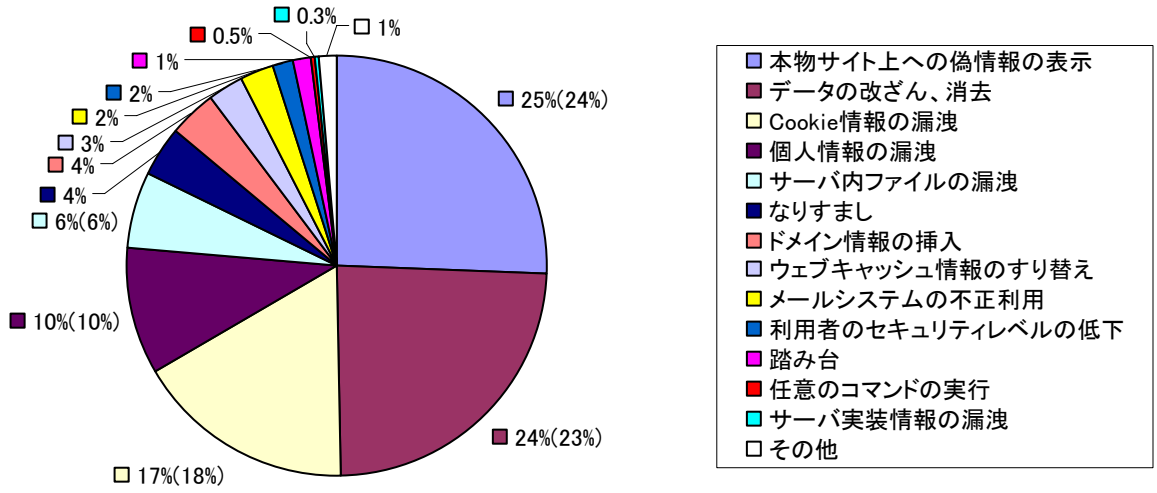


図 2-3. ウェブサイトの脆弱性種類別件数の推移（届出受付開始から 2007 年 3 月末まで）[3]

[3] 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。



（782 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 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 割近くをしめます（図 2-2）。

「クロスサイト・スクリプティング」が多く届けられたことから脆弱性の脅威としては「本物サイト上への偽情報の表示」が増え、「SQL インジェクション」の脅威である「データの改ざん、消去」よりも多くなっています（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 55%の届出が 30 日以内、全体の 81%の届出が 90 日以内に修正されています。

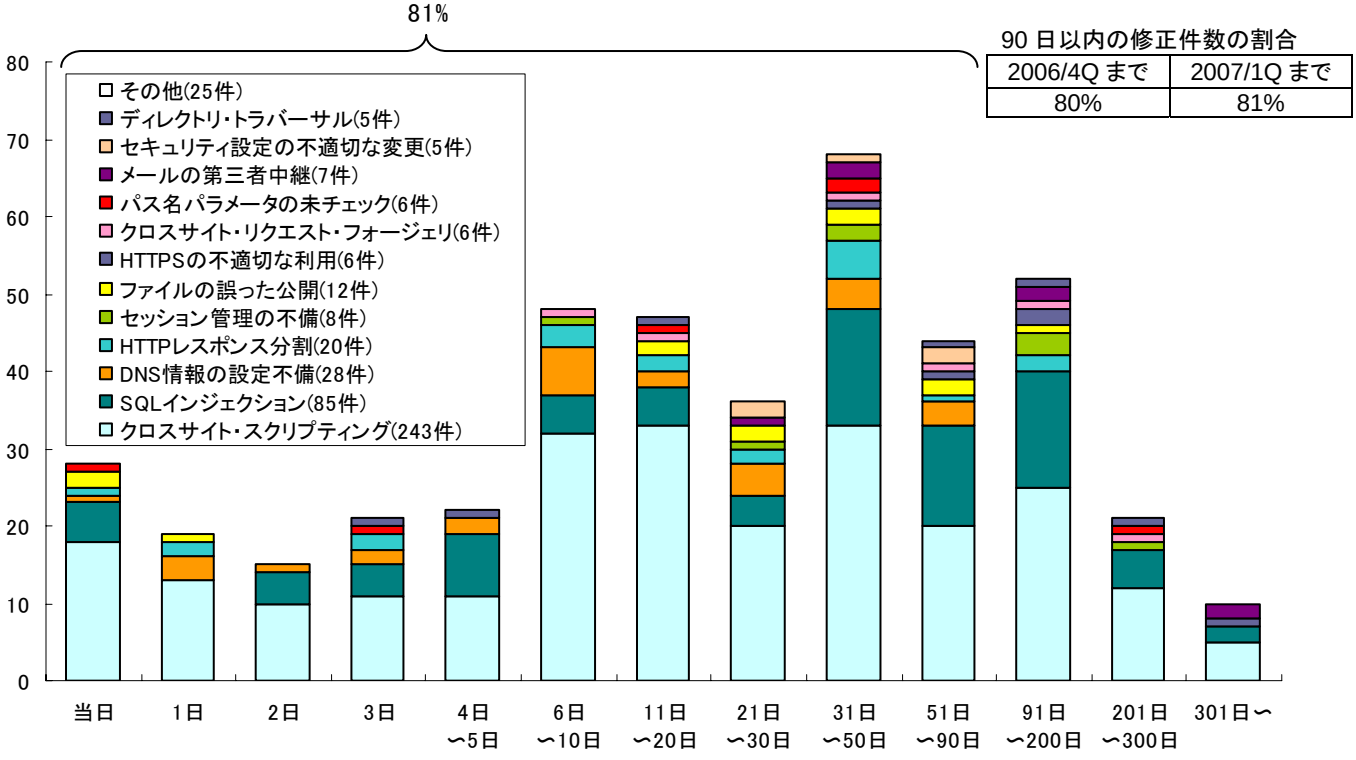


図 2-5. ウェブサイトの脆弱性修正に要した日数

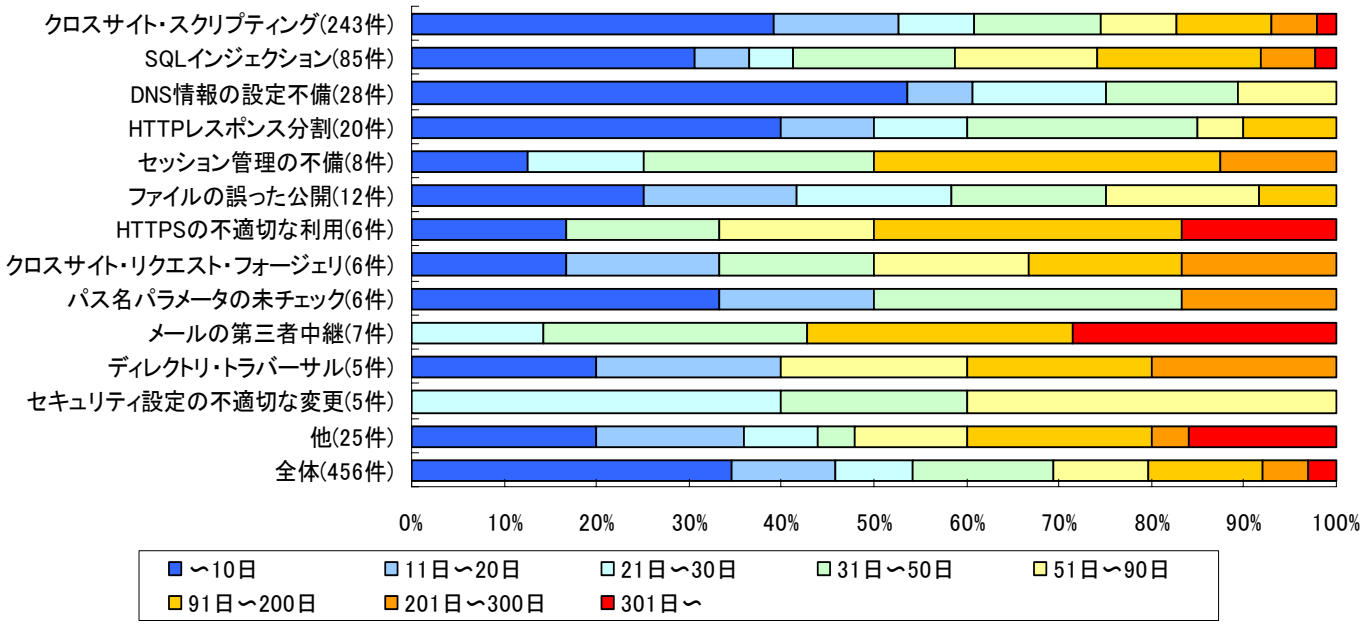


図 2-6. ウェブサイトの脆弱性修正に要した日数の傾向

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。

(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

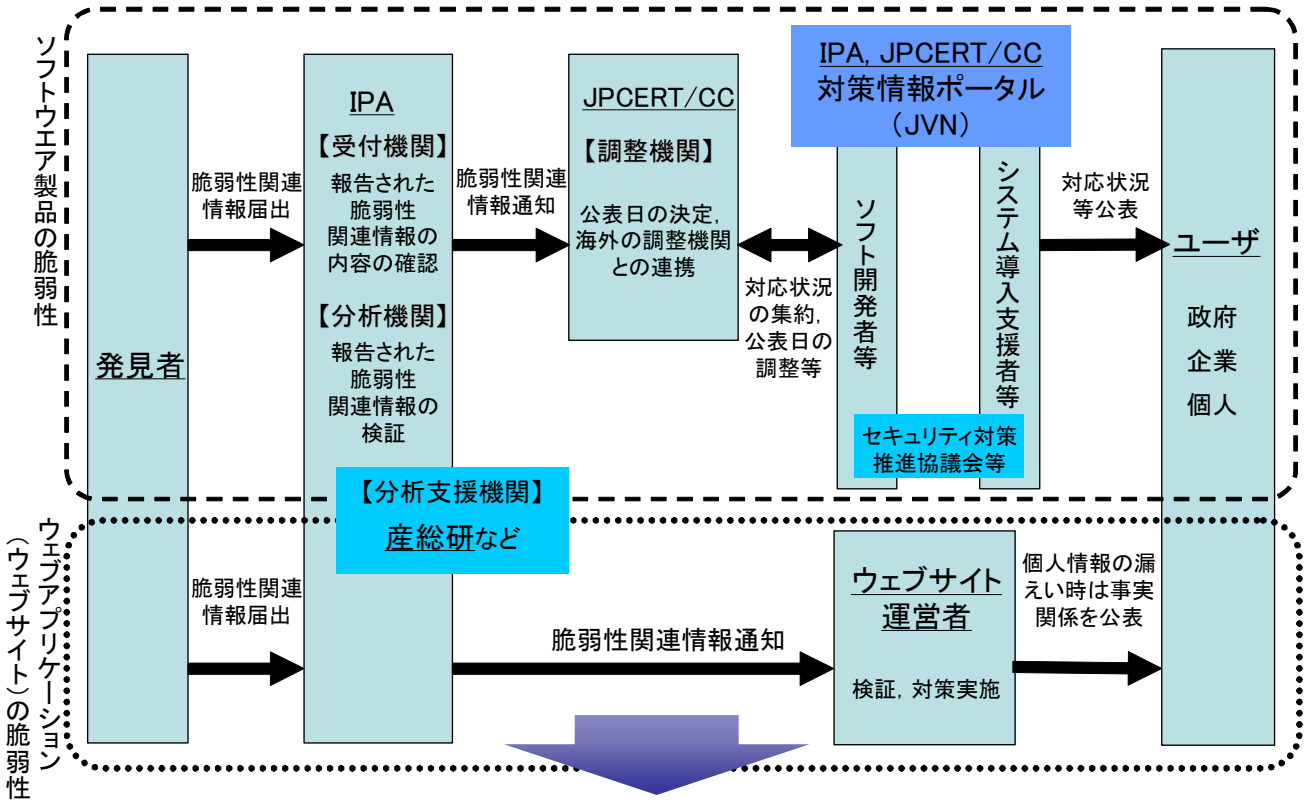
	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩

	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