プレスリリース
2006 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

ソフトウエア等の脆弱性関連情報に関する届出状況 [2006 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) 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) は、経済産業省告示に基づき、2004 年 7 月から脆弱性関連情報の取扱いを開始しています。IPA は脆弱性関連情報の届出受付、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。今般、2006 年第 2 四半期 (4 月～6 月) の脆弱性関連情報の届出状況を以下のとおり、とりまとめました。

要約

脆弱性関連情報の届出受付開始から 2 年が経過し、この間、合計 821 件の届出がありました。

- 今四半期のソフトウエア製品の脆弱性関連情報

  届出　　：84 件 (届出受付開始からの累計は 257 件)

  脆弱性公表：22 件 (届出受付開始からの累計は 89 件)

- 今四半期のウェブアプリケーションの脆弱性関連情報

  届出　　：57 件 (届出受付開始からの累計は 564 件)

  修正完了　：31 件 (届出受付開始からの累計は 297 件)

- 今四半期の特徴は以下の通りです。

ソフトウエア製品の届出が 84 件あり、過去最高を記録しました。特にオープンソースソフトウエア (OSS) に関する届出が 57 件あり、著しく増加しています。また、JVN[1]での脆弱性公表を 22 件行い、過去最高を記録しました。

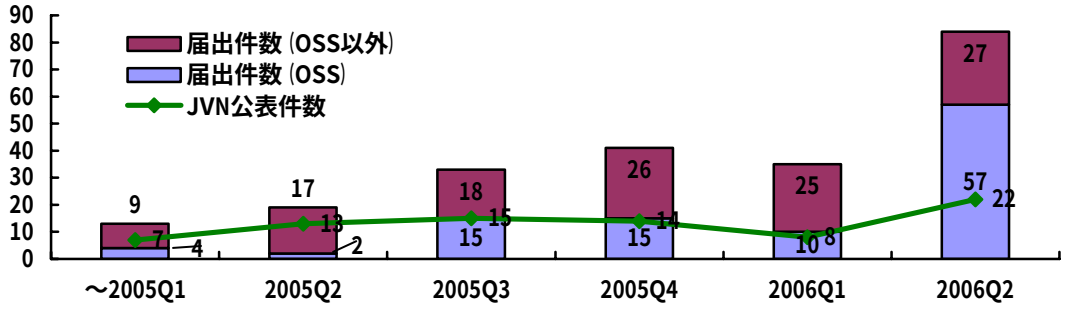


図　ソフトウエア製品の脆弱性 内訳 (届出受付開始から 2006 年 6 月末まで)

この間、JVN で公表したものとして、ファイル交換ソフト「Winny」のバッファオーバーフローの脆弱性 (p.6 表 2-2 項番 9) があります。IPA および JPCERT/CC はこの脆弱性を開発者に通知しましたが、修正方法が公表されませんでしたので、製品開発者の対応状況を JVN で公表しました。

また、OSS 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 12 件 (表 2-2 項番 6、7、8、10、13、14、15、16、17、18、21、22) ありました。

このほかに、製品開発者自身から連絡を受け、対策情報を公表したものが 3 件 (表 2-2 項番 12、13、14) ありました。対策を利用者へ周知徹底するために JVN を活用していただいたものと推測されます。

---

[1] IPA および JPCERT/CC が運営する脆弱性対策情報ポータルサイトです。製品開発者の脆弱性への対応状況を公表しています。脆弱性関連情報取扱いの枠組み「情報セキュリティ早期警戒パートナーシップ」の詳細は付録の図を参照してください。

1　届出件数[2]

2006 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、141 件（ソフトウエア製品に関するもの 84 件、ウェブアプリケーションに関するもの 57 件）であり、届出受付開始（2004 年 7 月 8 日）からの累計は 821 件（ソフトウエア製品に関するもの 257 件、ウェブアプリケーションに関するもの 564 件）です。四半期毎の届出状況を図 1-1 に示します。1 就業日あたりの届出件数は 1.70 件であり、前四半期より増加しています。

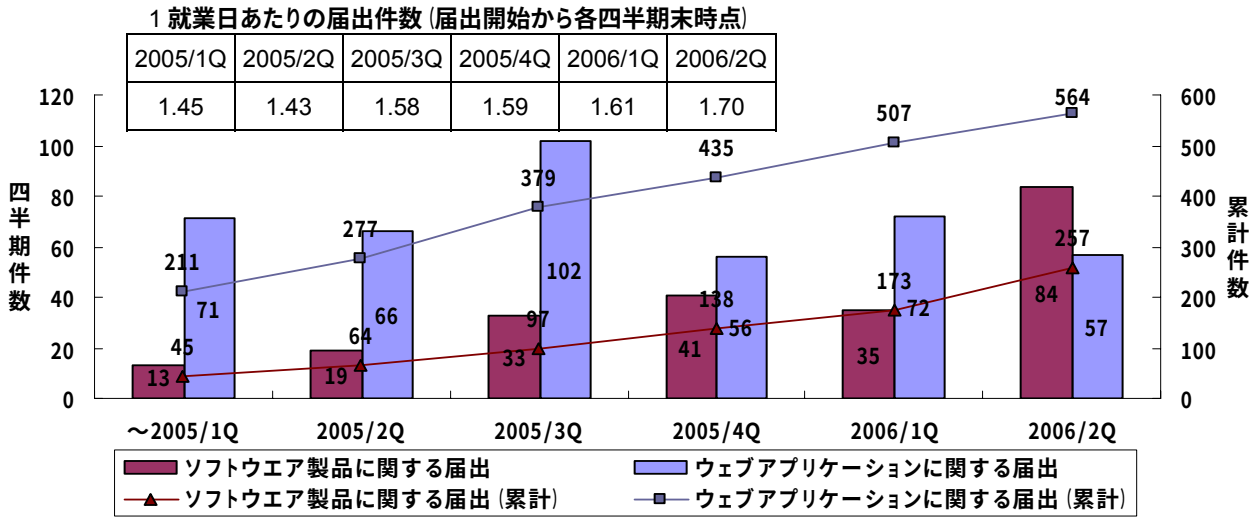
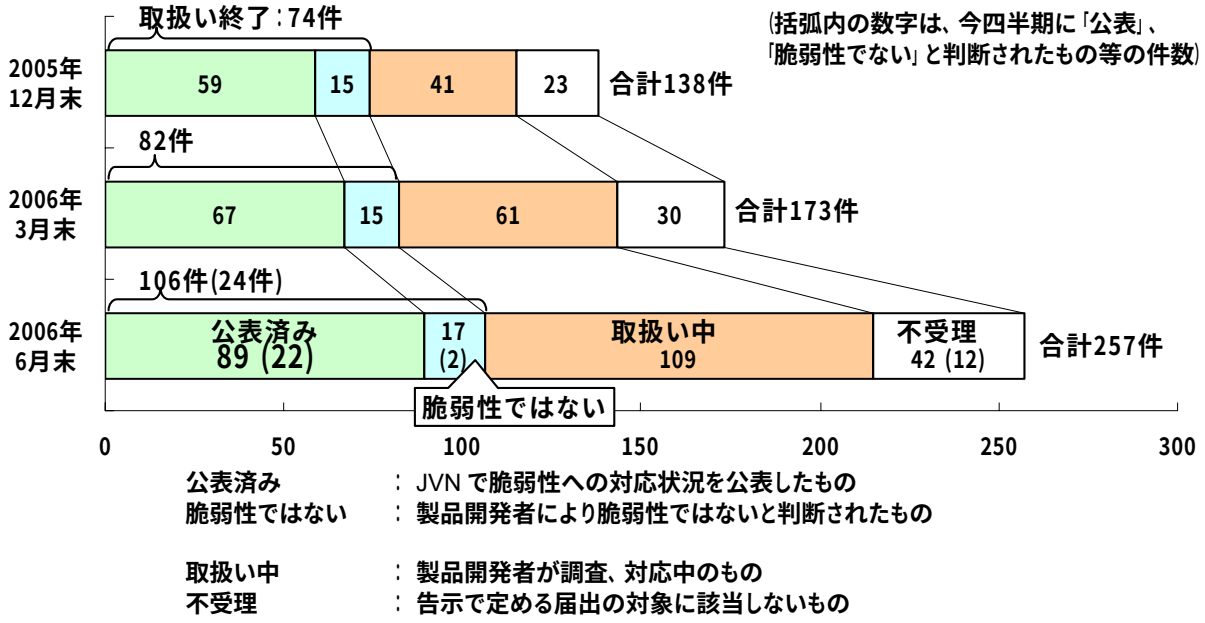


図 1-1 脆弱性関連情報の四半期別届出件数の推移

(1) ソフトウエア製品の脆弱性

ソフトウエア製品の脆弱性関連情報の届出について、処理状況を図 1-2 に示します。

図 1-2 に示すとおり、今四半期中に公表した脆弱性は、22 件（累計 89 件）です。また、「不受理」としたものは 12 件（累計 42 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 1-2 ソフトウエア製品 各時点における脆弱性関連情報の届出の処理状況

---

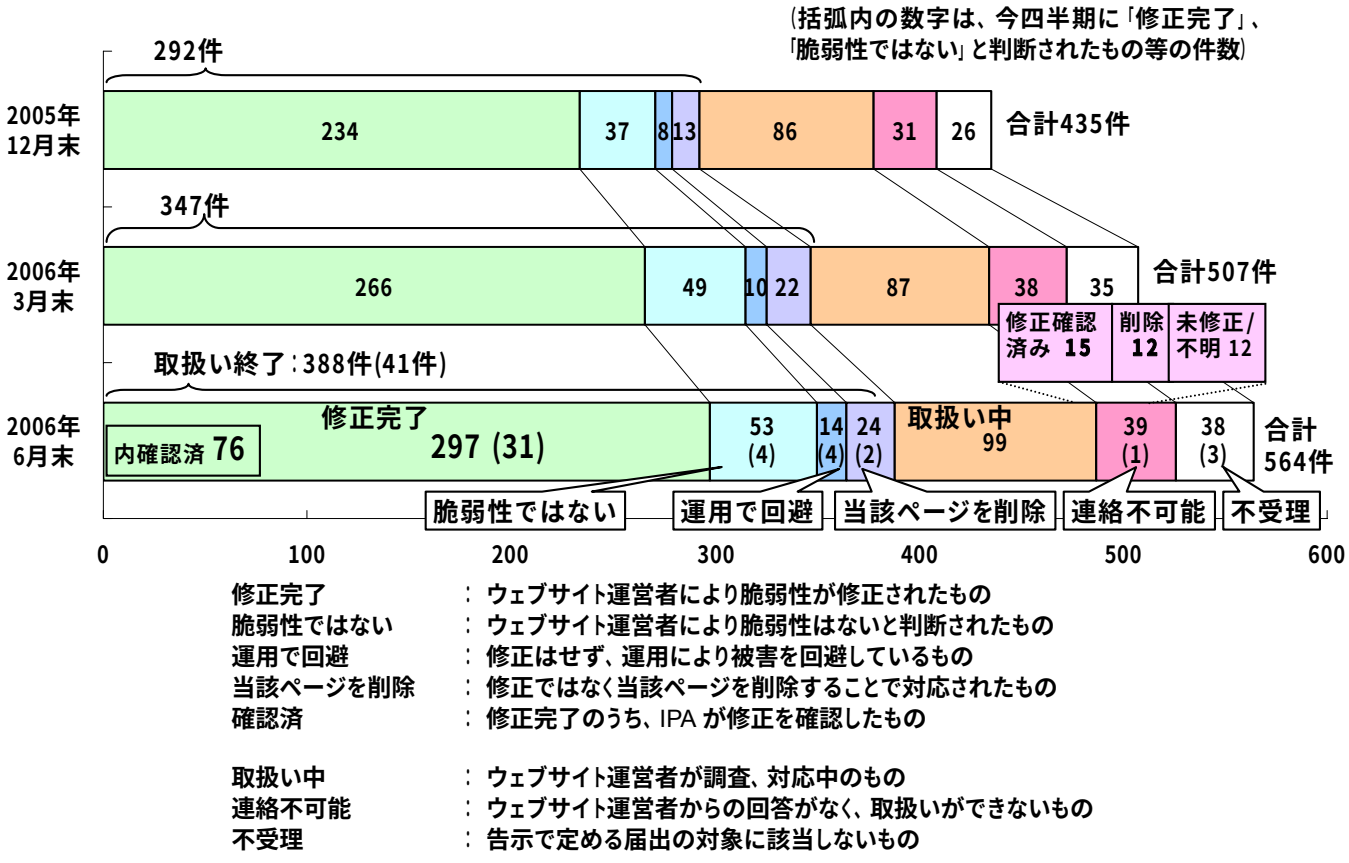
[2] ソフトウエア製品については、前四半期までは、国内の発見者から IPA に届出があったもののみを計上していましたが、今四半期からは、製品開発者自身から自社製品の脆弱性・対策方法について連絡を受けたものを加え、今四半期以前に遡って計上しています。

⑵ 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の脆弱性関連情報の届出について、処理状況を図 1-3 に示します。

図 1-3 に示すとおり、ウェブアプリケーション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 41 件（累計 388 件）でした。このうち、「修正完了」したものは 31 件（累計 297 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 4 件（累計 53 件）、脆弱性を「運用で回避」すると対応されたものが 4 件（累計 14 件）、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が 2 件（累計 24 件）ありました。「修正完了」したもののうち 7 件（累計 76 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 3 件（累計 38 件）ありました。「連絡不可能」の届出のうち、15 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、12 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 1-3 ウェブアプリケーション 各時点における脆弱性関連情報の届出の処理状況

2　ソフトウエア製品の脆弱性関連情報の取扱いおよび調整[2]

2.1　ソフトウエア製品の脆弱性情報

図 2-1 に、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エア製品の内訳を示します。2005Q3 からオープンソースソフトウエアに関する届出が増加しましたが今期は特に多く 57 件ありました。

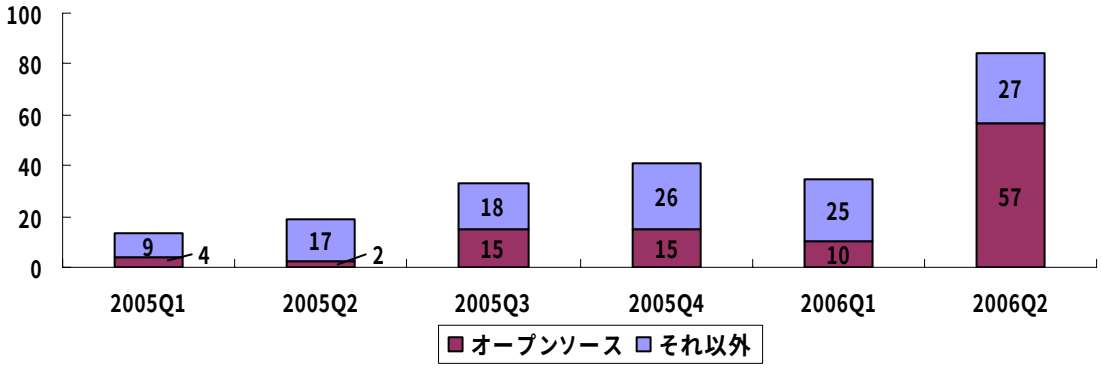
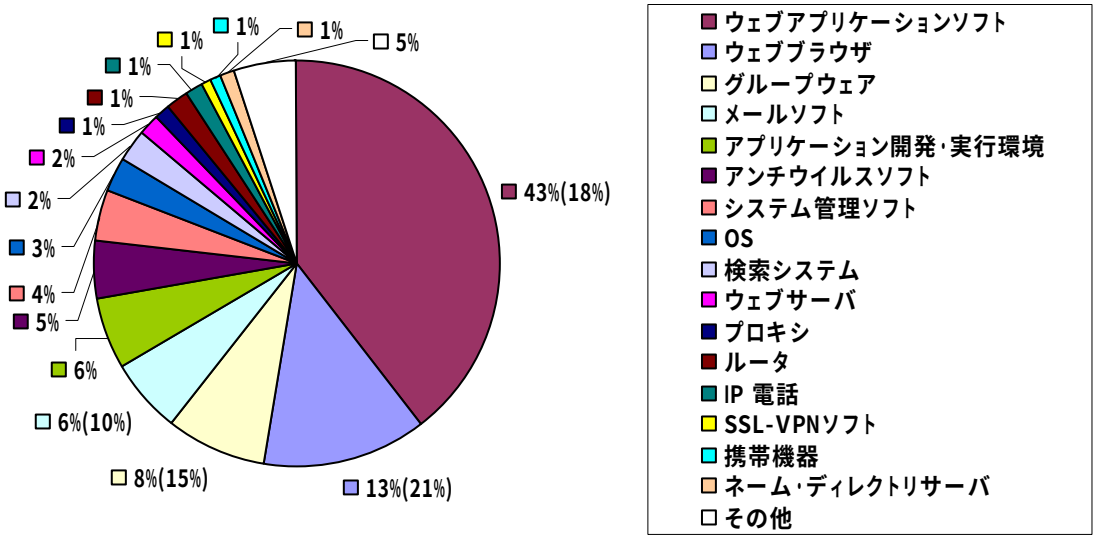


図 2-1　ソフトウエア製品の脆弱性 内訳（届出受付開始から 2006 年 6 月末まで）

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エア製品に関する脆弱性関連情報 257 件のうち、不受理のものを除いた 215 件の製品種類別の内訳を図 2-2 に、原因別の内訳を図 2-3 に、脅威別の内訳を図 2-4 に示します。



※その他には、情報家電、周辺機器、ファイル交換ソフト等があります

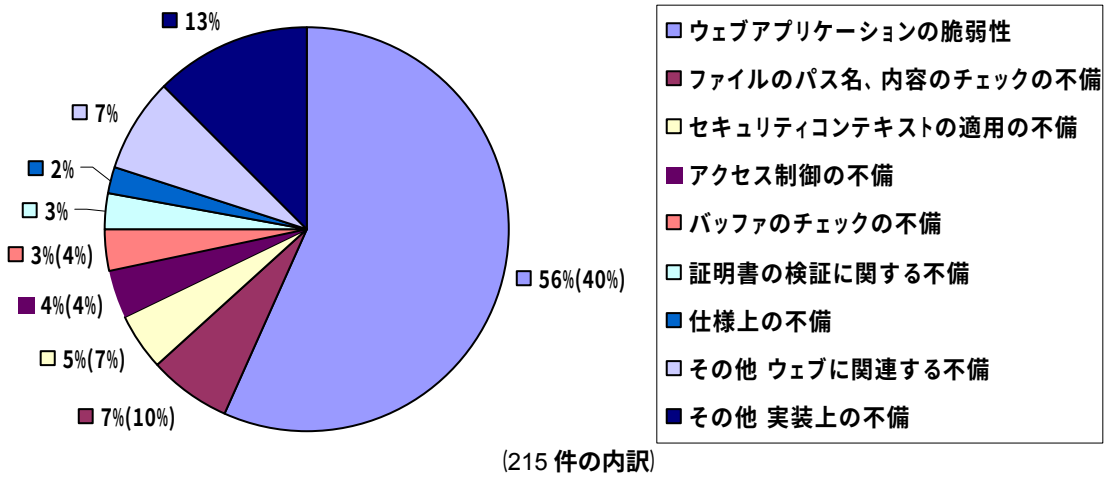
（215 件の内訳）　（グラフの括弧内は前四半期の数字）

図 2-2　ソフトウエア製品の脆弱性 製品種類別内訳（届出受付開始から 2006 年 6 月末まで）[3]

図 2-2 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エアだけでなく、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。

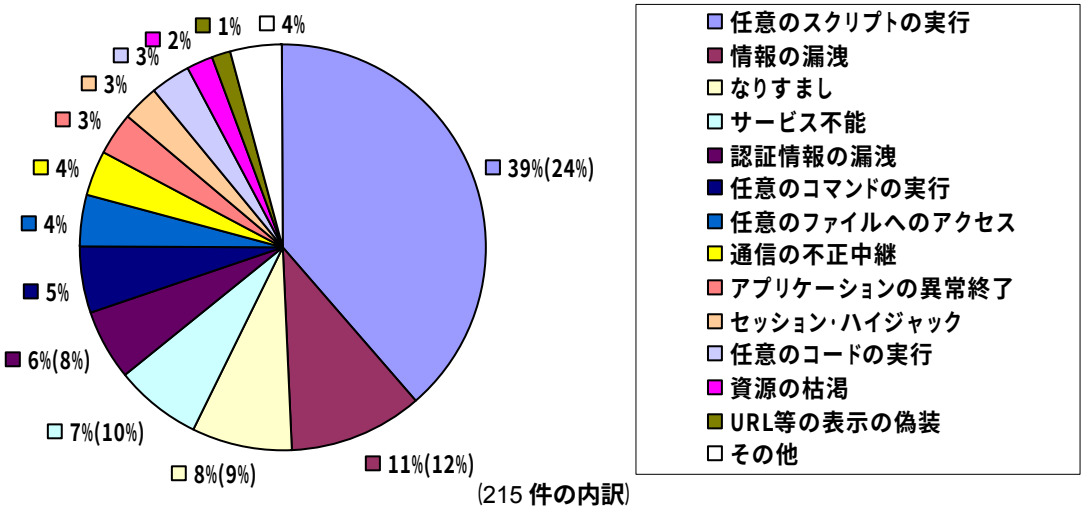
---

[3]前四半期まで使用していた「ウェブアプリ構築関係」の分類を見直し、「ウェブアプリケーションソフト」および「アプリケーション開発・実行環境」へ変更しました。前四半期まで使用していた「ミドルウェア」は「アプリケーション開発・実行環境」へ統合しました。



(215 件の内訳)

図 2-3　ソフトウエア製品の脆弱性 原因別内訳 (届出受付開始から 2006 年 6 月末まで) [4]



(215 件の内訳)

図 2-4　ソフトウエア製品の脆弱性 脅威別内訳 (届出受付開始から 2006 年 6 月末まで)

図 2-3 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 2-4 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」以外のソフトウエア製品であっても、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。

2.2　ソフトウエア製品の脆弱性情報の調整および公表状況

JPCERT/CC は、表 2-1 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[5]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/)。

---

[4] それぞれの脆弱性の詳しい説明については付録を参照してください。

[5] 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 2-1 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	22	89
②	海外 CSIRT から連絡を受けたもの	3	102
	計	25	191

(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 2006 年 6 月末までの届出について、脆弱性関連情報の届出 (表 2-1 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 2-5 に示します。全体の 48%の届出が 45 日以内に公表されています。

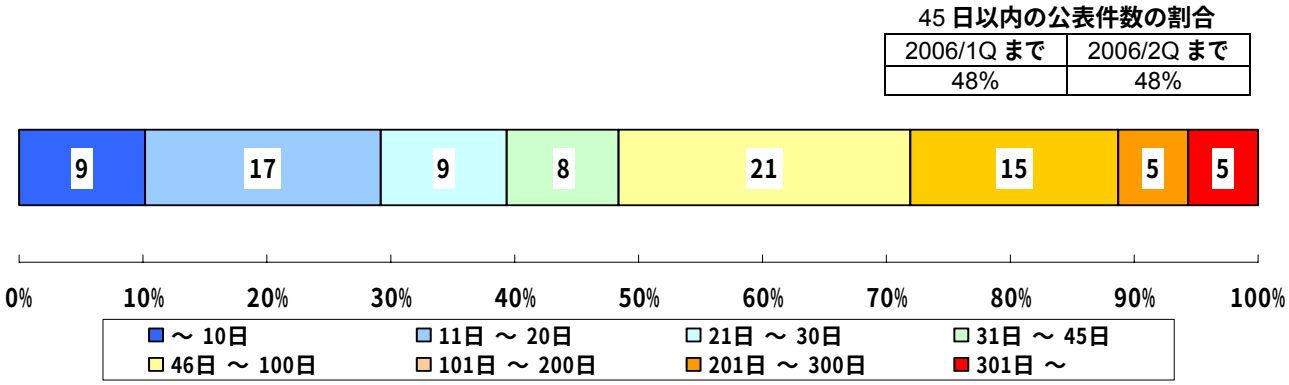


図 2-5 ソフトウエア製品の脆弱性 公表日数

表 2-2 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。

今四半期は、ファイル交換ソフト「Winny」におけるバッファオーバーフローの脆弱性 (表 2-2 項番 9) を公表しました。IPA および JPCERT/CC はこの脆弱性を開発者に通知しましたが、修正方法が公表されなかったため、注意喚起として、製品開発者の対応状況を JVN で公表しました。

複数の製品開発者のソフトウエア製品に影響がある脆弱性は、2 件 (項番 1、2) であり、特定の製品に関する脆弱性は 20 件でした。なお、12 件 (項番 6、7、8、10、13、14、15、16、17、18、21、22) はオープンソースソフトウエアに関して開発者、開発コミュニティに通知し、公表したものです。また、3 件 (項番 12,13,14) は製品開発者自身から脆弱性およびその対策情報の連絡を受け、公表したものです。

表 2-2 2006 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
複数開発者・製品に影響がある脆弱性	1	複数のメールクライアントソフトにおける、Unicode の取り扱い不備によるディレクトリ・トラバーサルの脆弱性	複数のメールクライアントソフトにおいて、添付ファイル名が Unicode で書かれている場合に文字列を適切に取り扱わない問題があります。このため、一見問題無く見える添付ファイルを開いた場合、予期せぬ場所にファイルが保存されてしまう可能性があります。	2006 年 5 月 9 日
	2	「Sun Java System Web Server」におけるクロスサイト・スクリプティングの脆弱性	「Sun Java System Web Server」には、Referer ヘッダを適切に取り扱わない問題があります。このため、第三者によりエラーページにスクリプトを埋め込まれる可能性があります。	2006 年 5 月 17 日

	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
特定製品の脆弱性	3	「CAFEMILK ショッピングカート CGI」におけるクロスサイト・スクリプティングの脆弱性	「CAFEMILK ショッピングカート CGI」は、利用者からの入力情報を確認画面に表示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。	2006 年 4 月 10 日
	4	「QUICK CART」におけるクロスサイト・スクリプティングの脆弱性	ショッピングカート「QUICK CART」は、利用者からの入力情報を確認画面に表示する際の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。	2006 年 4 月 13 日
	5	「QUICK CART」における OS コマンドインジェクションの脆弱性	ショッピングカート「QUICK CART」は、メールを送信する際の処理に問題があります。このため、遠隔の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。	2006 年 4 月 13 日
	6 (*1)	「FreeStyleWiki」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ上からウェブコンテンツの発行や編集を行える「FreeStyleWiki」には、ウェブコンテンツ編集時の内容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。	2006 年 4 月 17 日
	7 (*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、利用者が編集したウェブコンテンツ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。	2006 年 4 月 19 日
	8 (*1)	「SquirrelMail」におけるクロスサイト・スクリプティングの脆弱性	ウェブメールクライアント「SquirrelMail」には、HTML メールをウェブページに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、HTML メールにスクリプトを埋め込まれる可能性があります。	2006 年 4 月 21 日
	9	「Winny」におけるバッファオーバーフローの脆弱性	ファイル交換ソフト「Winny」は、通信処理にバッファオーバーフローの脆弱性があります。	2006 年 4 月 21 日
	10 (*1)	「Apache Struts」において Validator による入力値検査が回避される脆弱性	ウェブアプリケーション開発支援フレームワーク「Apache Struts」の Validator 機能には、細工されたリクエストにより入力値検査を回避されてしまう問題があります。このため、Validator を実装しているウェブアプリケーションが、想定外の入力値を受け取ってしまう可能性があります。	2006 年 4 月 26 日

	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
特定製品の脆弱性（続き）	11	「DonutP」および「UnDonut」における確認ダイアログ表示に関する脆弱性	タブ型ウェブブラウザ「DonutP」およびその後継である「UnDonut」には、通常のスクリプトよりも機能を拡張した操作を行う API 関数を呼び出す際に、確認ダイアログを表示しない問題があります。	2006 年 4 月 27 日
	12 (*2)	「MyWeb」における SQL インジェクションの脆弱性	グループウェア「MyWeb」の一部の機能に SQL インジェクションの脆弱性が存在します。このため、遠隔の第三者により、データベース内容の改ざんやデータの盗難などが行なわれる可能性があります。	2006 年 5 月 22 日
	13 (*1) (*2)	「RWiki」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ上からウェブコンテンツの発行や編集を行える「RWiki」は、コンテンツを表示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。	2006 年 5 月 24 日
	14 (*1) (*2)	「RWiki」において任意の Ruby スクリプトを実行される脆弱性	ウェブブラウザ上からウェブコンテンツの発行や編集を行える「RWiki」には、編集画面において任意の Ruby スクリプトが実行可能な脆弱性が存在します。	2006 年 5 月 24 日
	15 (*1)	「Mozilla Firefox」において HTTP 1.0 解釈に関してレスポンス分割が可能な脆弱性	ウェブブラウザ「Mozilla Firefox」は、サーバからの HTTP 1.0 応答（レスポンス）を適切に取扱わないため、レスポンス分割攻撃を受ける問題があります。このため、利用者が複数のウェブサイトを同時に閲覧していると、サイトの表示内容を改ざんされる可能性があります。	2006 年 6 月 2 日
	16 (*1)	「Mozilla Firefox」において HTTP ヘッダ名解釈に関してレスポンス分割が可能な脆弱性	ウェブブラウザ「Mozilla Firefox」は、サーバからの HTTP 応答（レスポンス）に含まれるヘッダの処理が適切でないため、レスポンス分割攻撃を受ける問題があります。このため、利用者が複数のウェブサイトを同時に閲覧していると、サイトの表示内容を改ざんされる可能性があります。	2006 年 6 月 2 日
	17 (*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「dotProject」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。	2006 年 6 月 5 日
	18 (*1)	CGI RESCUE 製「WebFORM」においてメールの不正送信が可能な脆弱性	フォームメール「WebFORM」には、メールのヘッダ部分へ挿入される入力値の検査が適切に行なわれません。このため、任意の宛先へのメールの送信に利用される可能性があります。	2006 年 6 月 9 日

	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
特定製品の脆弱性（続き）	19	「Internet Explorer」におけるアドレスバー偽装の脆弱性	ウェブブラウザ「Internet Explorer」には、実際にアクセスしているものとは異なる URL をアドレスバーに表示してしまう問題があります。	2006 年 6 月 14 日
	20	「Webmin」におけるディレクトリ・トラバーサルの脆弱性	Unix のシステム管理をウェブブラウザから行うためのインターフェース「Webmin」には、ディレクトリ・トラバーサルによって認証を回避されてしまう問題があります。	2006 年 6 月 23 日
	21 (*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「dotProject」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。	2006 年 6 月 26 日
	22 (*1)	「Phorum」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウエア「Phorum」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。	2006 年 6 月 26 日

(*1) オープンソースソフトウエアの脆弱性

(*2) 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

⑵ 海外 CSIRT から連絡を受け公表した脆弱性

表 2-3、表 2-4 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 2 件、英国 NISCC（National Infrastructure Security Co-ordination Centre）から 1 件の合計 3 件の脆弱性関連情報の連絡を受けました。このほか、10 件の US-CERT Technical Cyber Security Alert を JVN で公表しました。

表 2-3 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	RealVNC Server に認証回避が可能な脆弱性	注意喚起として掲載[6]
2	Sendmail における マルチパート MIME メッセージ処理に関する脆弱性	複数製品開発者へ通知

表 2-4 NISCC から連絡を受けた脆弱性関連情報および対応状況

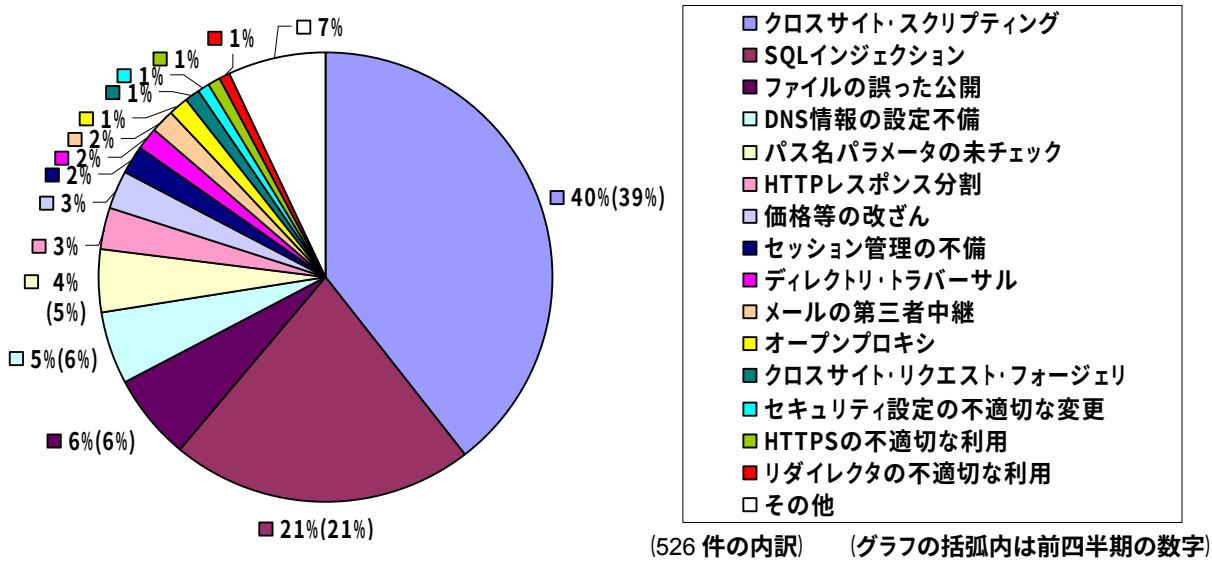
項番	脆弱性	対応状況
1	DNS プロトコルの実装における脆弱性	複数製品開発者へ通知

[6]国内の製品開発者へ通知・調整はしていませんが、国内で広く利用されているため、注意喚起として JVN に掲載しました。

3　ウェブアプリケーションの脆弱性関連情報の取扱い

3.1　ウェブアプリケーションの脆弱性情報

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アプリケーションの脆弱性関連情報564件のうち、不受理のものを除いた526件の種類別内訳を図3-1に、脅威別内訳を図3-2に示します。

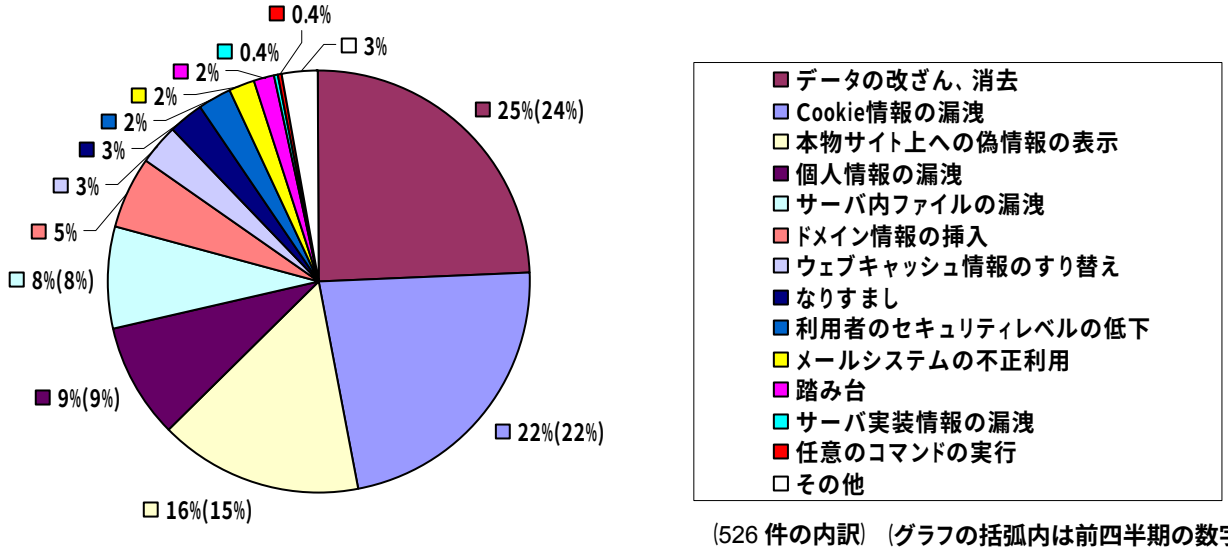


(526件の内訳)　(グラフの括弧内は前四半期の数字)

図 3-1　ウェブアプリケーションの脆弱性種類別内訳(届出受付開始から2006年6月末まで)[4]

図3-1に示すように、脆弱性の種類は、依然として「クロスサイト･スクリプティング」、「SQLインジェクション」が多くあります。

「SQLインジェクション」の届出の多くは、データベースのエラーメッセージが表示されたページを発見したというものです。これまでに取扱いを終了した77件のうち、47件は「SQLインジェクション」の問題が実際にあり修正したとの報告を受け、残りの30件はエラーメッセージが表示されていただけで実際にはSQLコマンドを挿入することはできず、「SQLインジェクション」の問題はなかったとの報告を受けました。



(526件の内訳)　(グラフの括弧内は前四半期の数字)

図 3-2　ウェブアプリケーションの脆弱性脅威別内訳(届出受付開始から2006年6月末まで)

図3-3に示すように、発見者が届出時に想定した脅威別では、「SQLインジェクション」により起こりうる「データの改ざん、消去」が最多であり、次いで「クロスサイト･スクリプティング」により起こりうる「Cookie情報の漏洩」「本物サイト上への偽情報の表示」があります。

3.2　ウェブアプリケーションの脆弱性の修正状況

届出受付開始から 2006 年 6 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 3-3 および図 3-4 に示します。全体の 80%の届出が、90 日以内に修正されています。

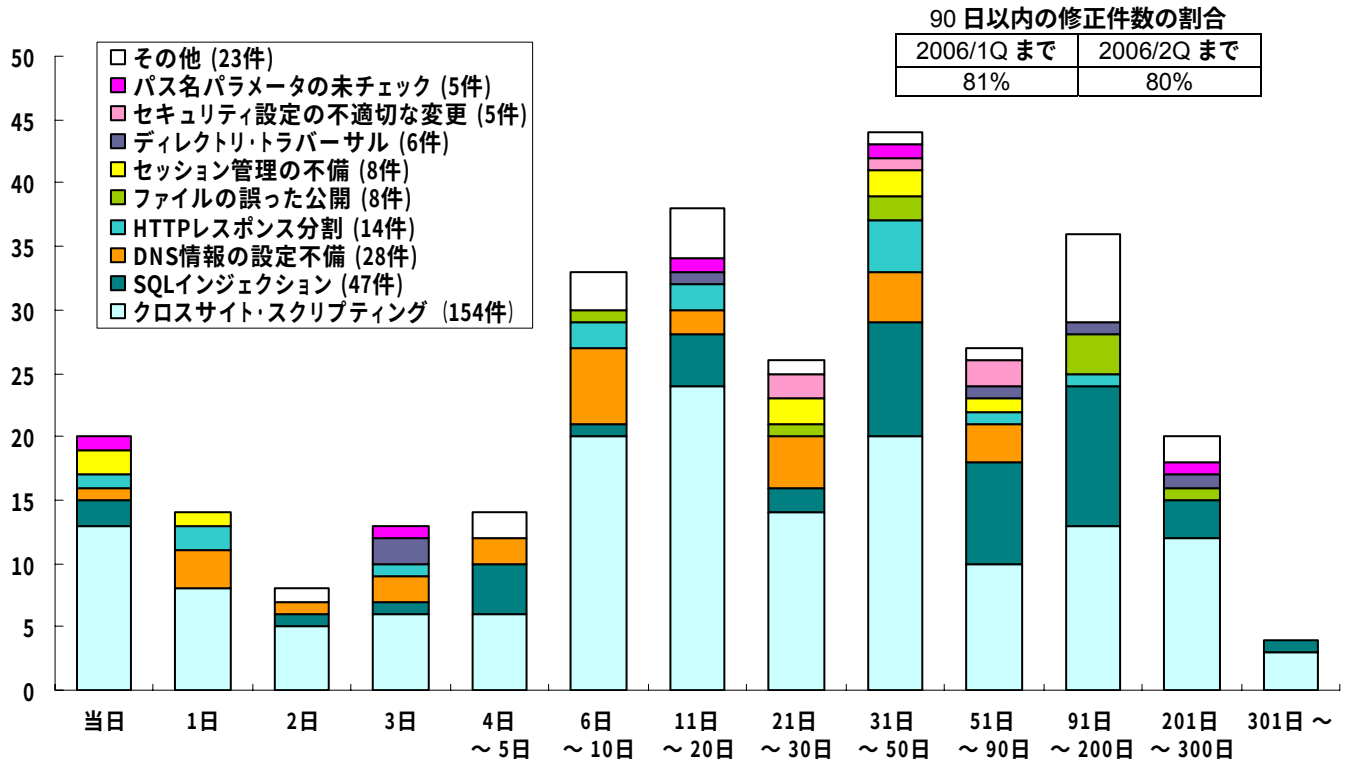


図 3-3　ウェブアプリケーションの脆弱性修正に要した日数

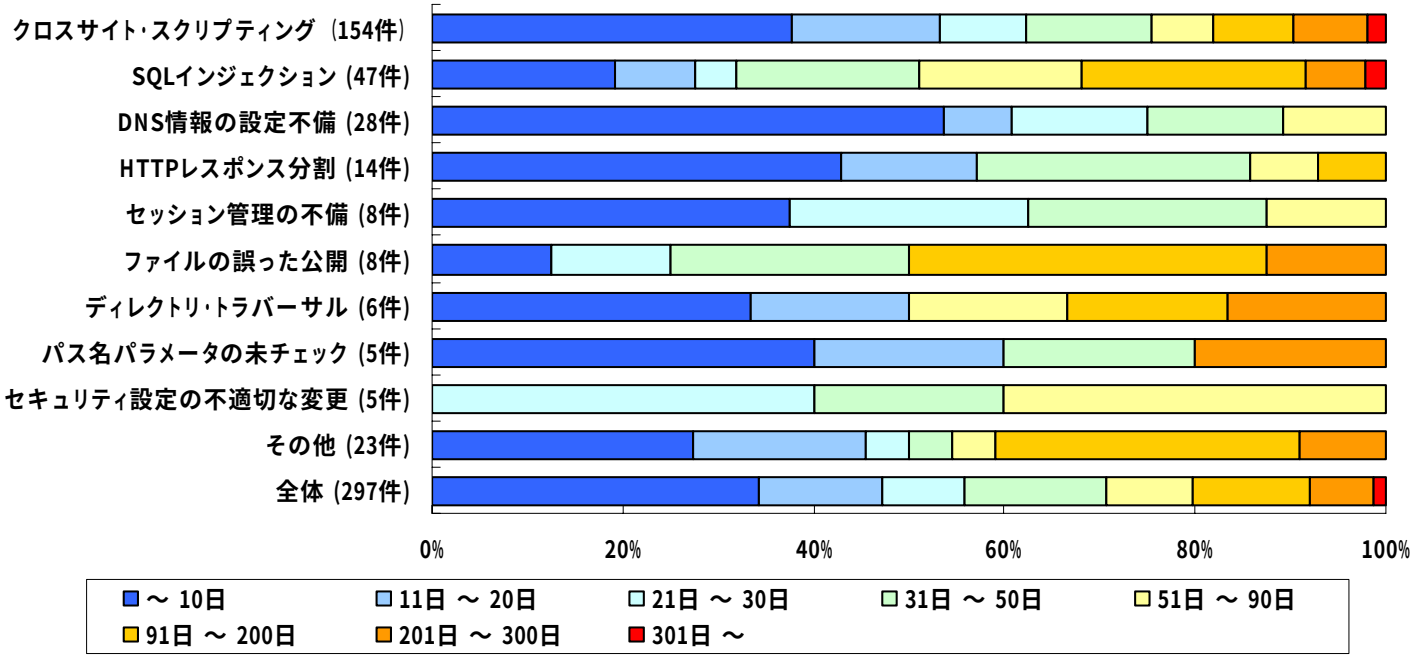


図 3-4　ウェブアプリケーションの脆弱性修正に要した日数の傾向

4　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。

- ウェブサイト運営者の皆様へ

  多くのウェブアプリケーションのソフトウエ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エ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。

- 製品開発者の皆様へ

  JPCERT/CC は、ソフトウエ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。

- 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エアを使い続けることは避けましょう。

■ 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

付表 1 ソフトウエア製品 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、入力された情報のチェックや内容の解釈、認証情報の取扱いに問題がある。「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

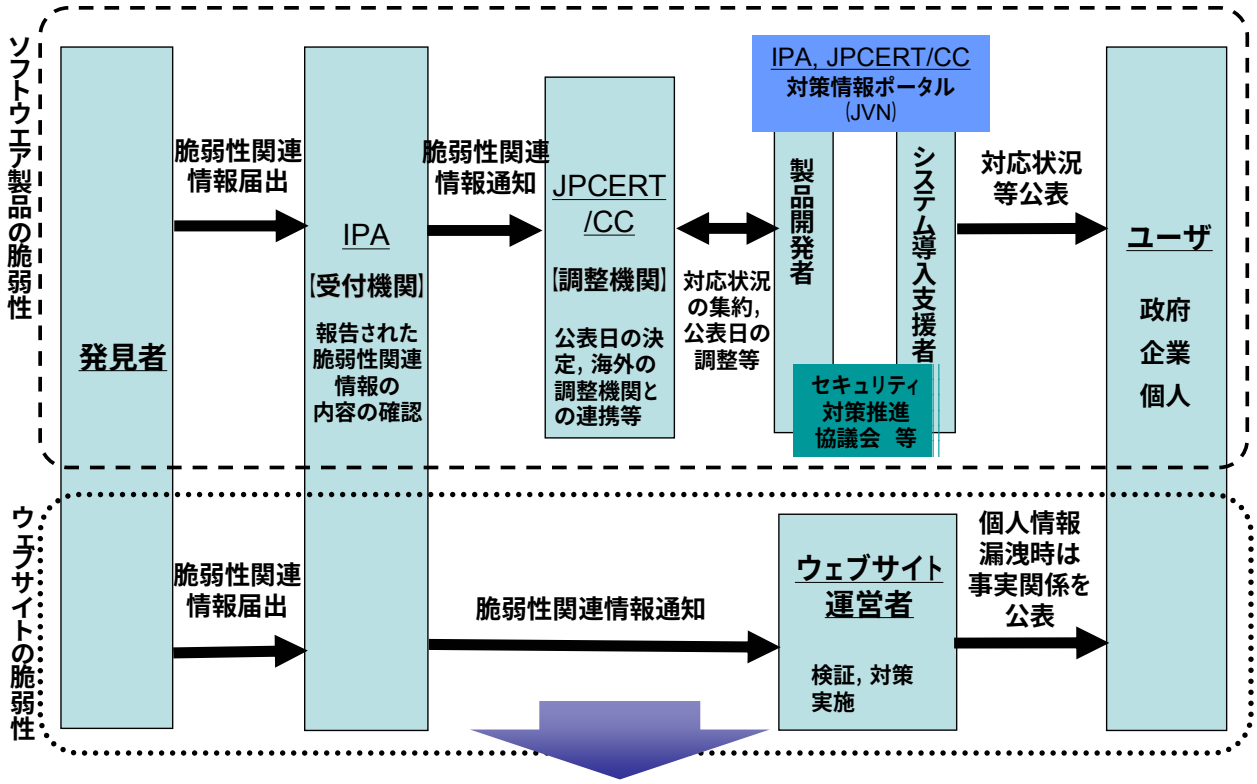
付表 2 ウェブアプリケーション脆弱性の分類

	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、ソフトウエ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

	脆弱性の種類	深刻度	説明	届出において想定された脅威
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	メールの第三者中継	低	他人のメールサーバを用いることで、自分の身元を隠してメールを送信することができる	メールシステムの不正利用
14	HTTPS の不適切な利用	低	HTTPS による暗号化をしているが、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
15	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

「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