プレスリリース
2006 年 10 月 17 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 3 四半期 (7 月～9 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、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 3 四半期 (7 月～9 月) の脆弱性関連情報の届出状況をとりまとめました。

1. 今四半期の届出件数

(1)今四半期のソフトウエア製品の脆弱性関連情報
・届出　　：37 件 (届出受付開始からの累計は 294 件)
・脆弱性公表：28 件 (届出受付開始からの累計は 117 件)
(2)今四半期のウェブアプリケーション (ウェブサイト) の脆弱性関連情報
・届出　　：97 件 (届出受付開始からの累計は 661 件)
・修正完了　：54 件 (届出受付開始からの累計は 351 件)

2. 今四半期までの届出状況

2004 年 7 月 8 日に脆弱性関連情報の届出受付を開始してから 2 年 3 ヶ月が経過し、今四半期までにソフトウエア製品に関するもの 294 件、ウェブアプリケーション (ウェブサイト) に関するもの 661 件、累計 955 件の届出がありました (図 1)。第 4 四半期には 1,000 件を超えるものと見込まれます。

発見者が届出時に想定した脅威別に内訳をすると、ソフトウエア製品に関しては「任意のスクリプト(*1)の実行 (41%)」、「情報の漏えい (10%)」、「なりすまし (8%)」が上位を占めています (図 2)。また、ウェブアプリケーション (ウェブサイト) に関しては「データの改ざん、消去 (25%)」、「本物サイト上への偽情報の表示 (20%)」、「Cookie(*2)情報の漏えい (20%)」が上位を占めています (図 3)。

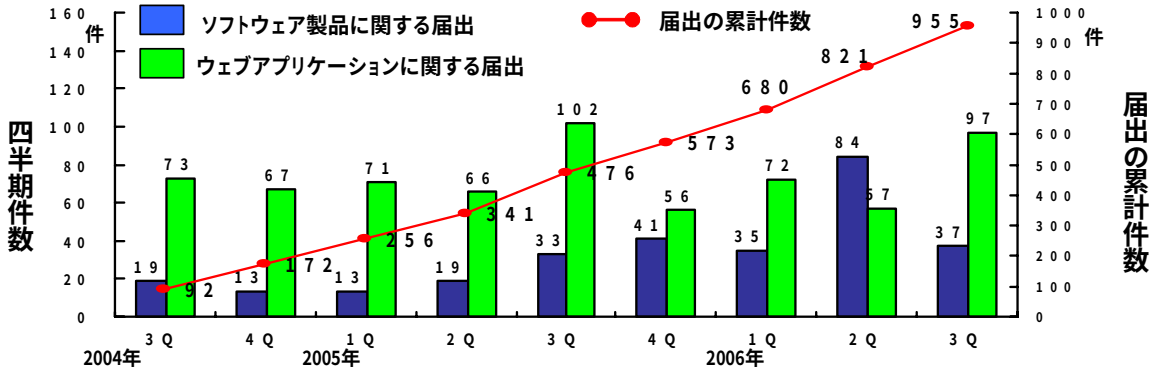


図1.脆弱性の届出件数の四半期別推移

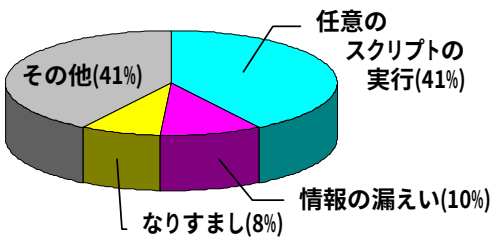


図2.ソフトウェア製品の脆弱性 (脅威別内訳)

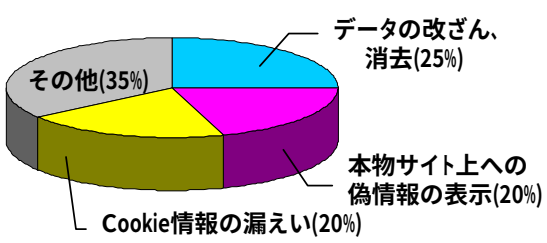


図3.ウェブアプリケーションの脆弱性 (脅威別内訳)

IPA では、届出件数の多い脆弱性を取り上げ、脆弱性の原因そのものをなくす根本的な解決策と、攻撃による影響の低減を期待できる保険的な対策を示した「安全なウェブサイトの作り方」を公表(*3)しています。本資料がウェブサイトのセキュリティ問題の解決の一助となれば幸いです。

(*1)：スクリプト

機械語へと変換する作業を省略して実行できるようにした簡易プログラム（通常のプログラムは、コンピュータが理解できる機械語へ変換してから実行される）。スクリプト言語には、JavaScript や VBScript などがある。

(*2)：Cookie

Web サーバと Web ブラウザとの間で、ユーザに関する情報やアクセス情報などをやりとりするための仕組み。「クッキー」と呼ぶ。

(*3)：「安全なウェブサイトの作り方」

http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

■ 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: ipa-pr@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. 届出状況

2006 年 7 月 1 日から 9 月 30 日までの IPA への脆弱性関連情報の届出件数は、134 件（ソフトウエア製品に関するもの 37 件、ウェブアプリケーションに関するもの 97 件）であり、届出受付開始（2004 年 7 月 8 日）からの累計は 955 件（ソフトウエア製品に関するもの 294 件、ウェブアプリケーションに関するもの 661 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 1.75 件であり、前四半期より増加しています。

1 就業日あたりの届出件数（届出開始から各四半期末時点）

2005/2Q	2005/3Q	2005/4Q	2006/1Q	2006/2Q	2006/3Q
1.43	1.58	1.59	1.61	1.70	1.75

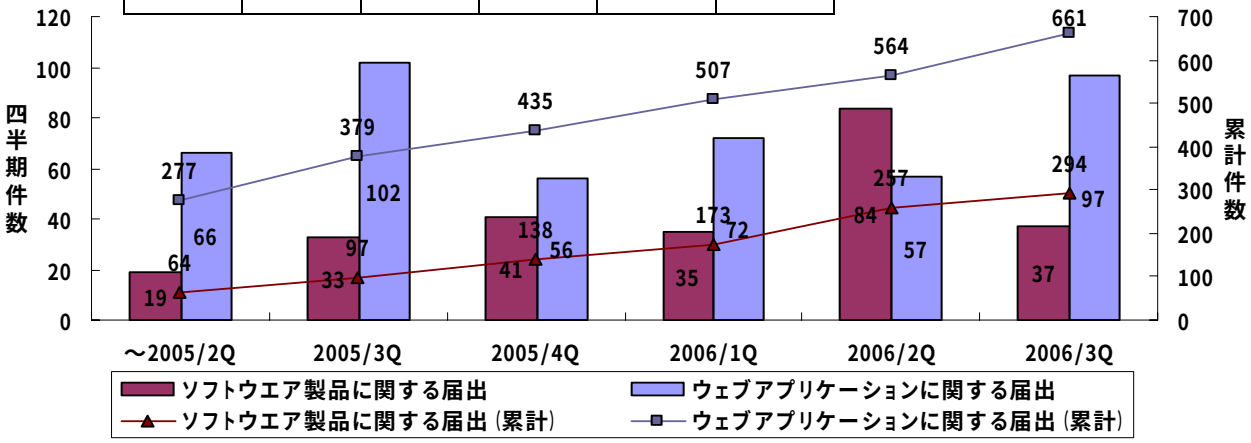
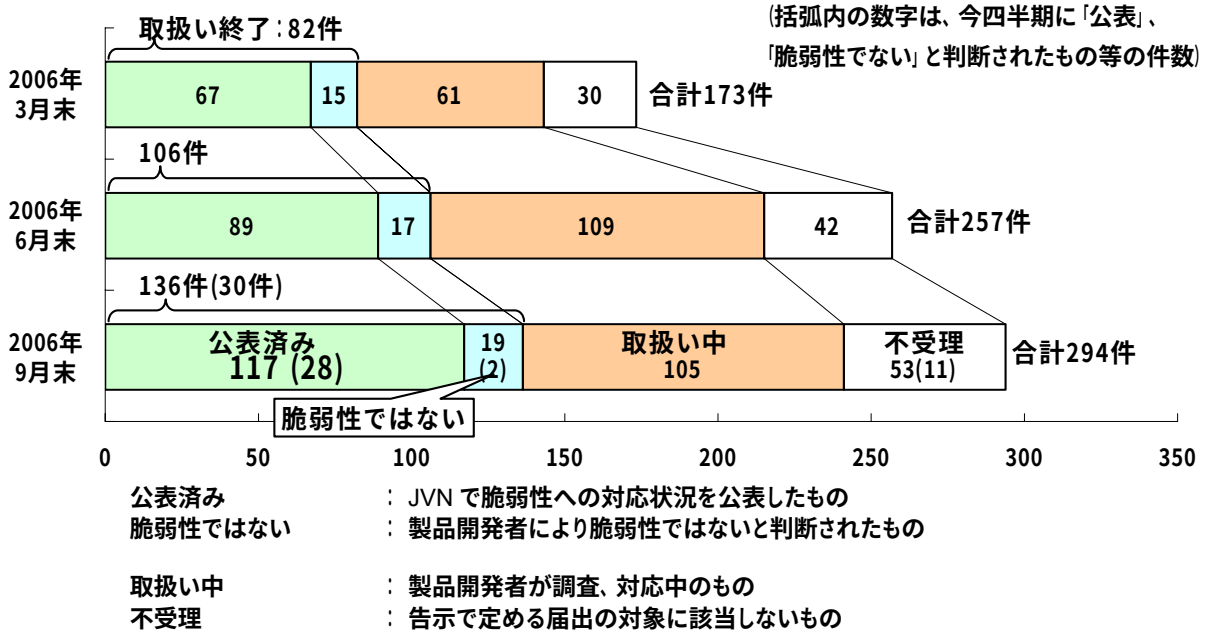


図 1-1 脆弱性関連情報の四半期別届出件数の推移

(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、28 件（累計 117 件）です。また、「不受理」としたものは 11 件（累計 53 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

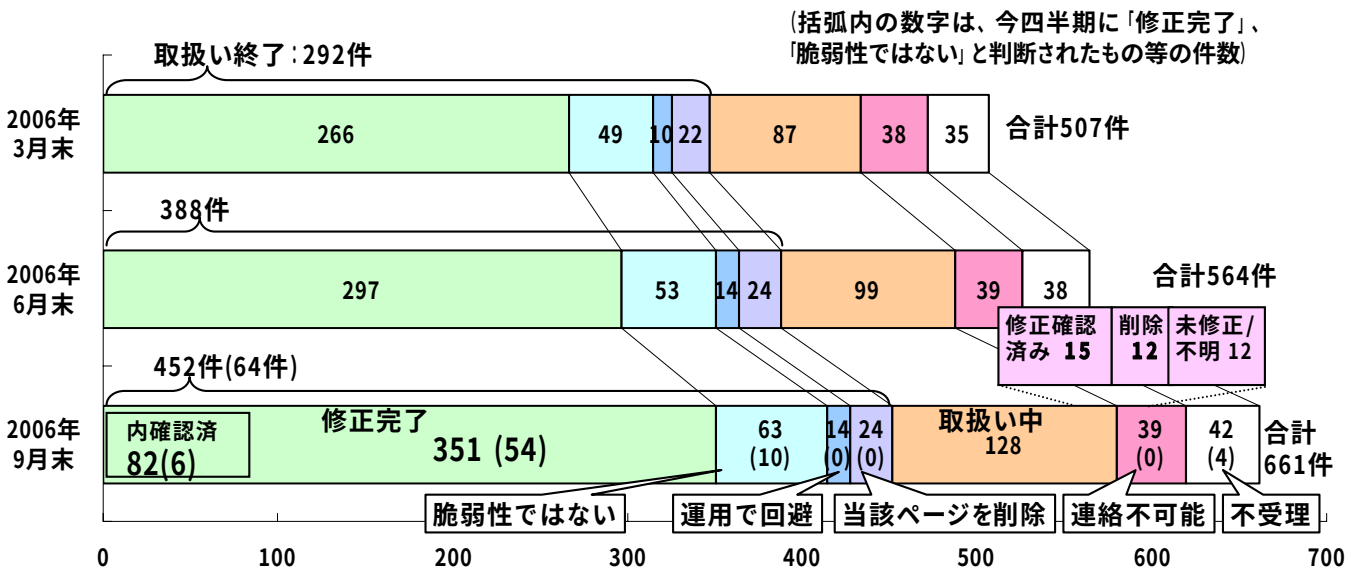
図 1-2 ソフトウエア製品 各時点における脆弱性関連情報の届出の処理状況

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 64 件（累計 452 件）でした。このうち、「修正完了」したものは **54** 件（累計 **351** 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 10 件（累計 63 件）ありました。「修正完了」したもののうち の 6 件（累計 **82** 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 4 件（累計 42 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

2.1 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ており、今期は 20 件ありました。

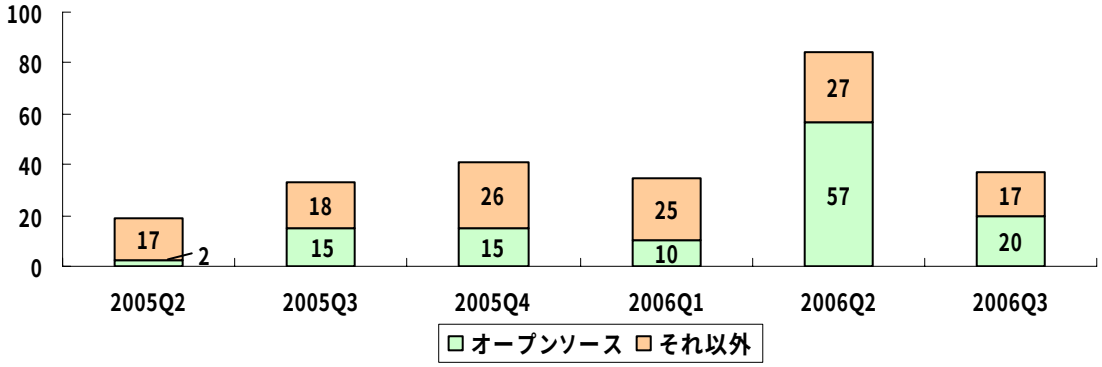
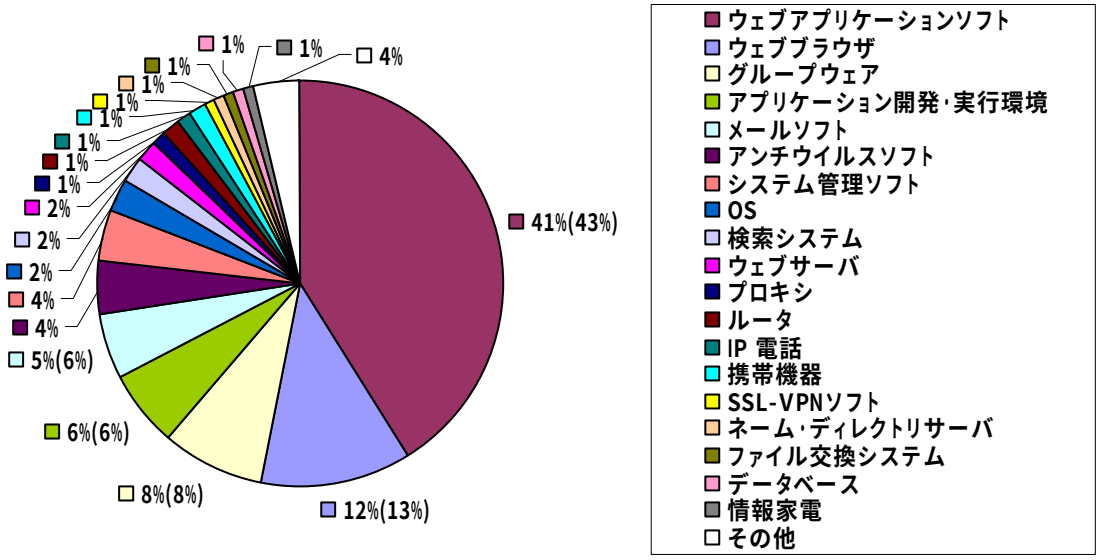


図 2-1 ソフトウエア製品の脆弱性 内訳 (届出受付開始から 2006 年 9 月末まで)

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 294 件のうち、不受理のものを除いた 241 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。

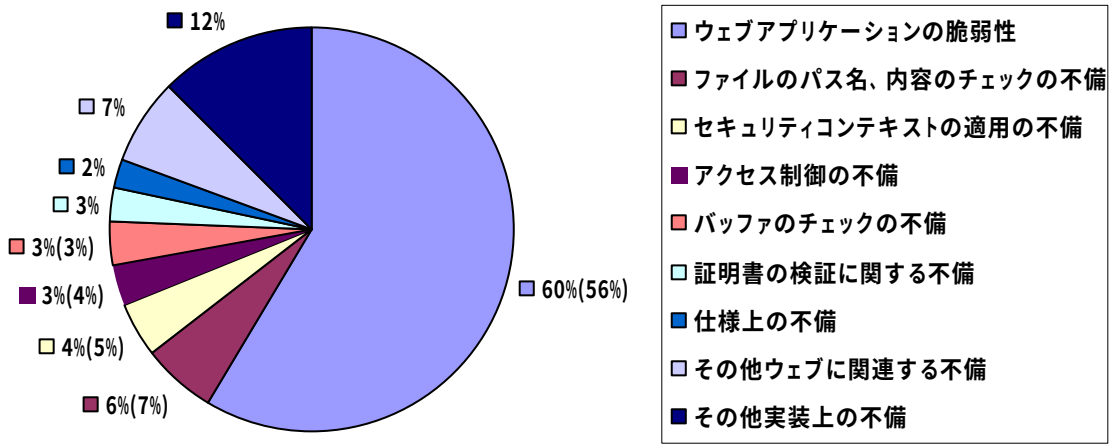


※その他には、周辺機器、ワープロソフト等があります

(241 件の内訳、グラフの括弧内は前四半期の数字)

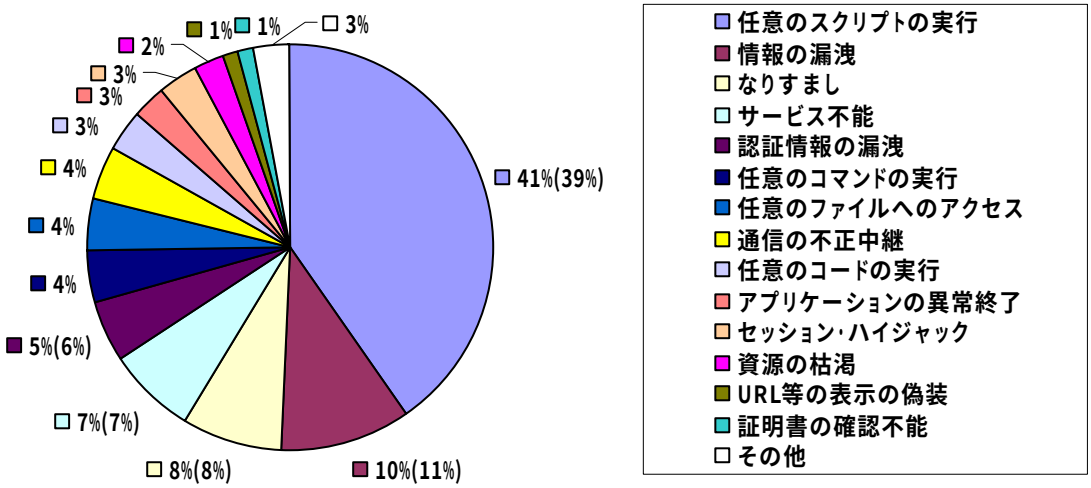
図 2-2 ソフトウエア製品の脆弱性 製品種類別内訳 (届出受付開始から 2006 年 9 月末まで)

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。



(241 件の内訳、グラフの括弧内は前四半期の数字)

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 9 月末まで) [1]



(241 件の内訳、グラフの括弧内は前四半期の数字)

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 9 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。

今期、製品開発者により脆弱性でないと判断された届出として、「XOOPS において、セッション ID の固定化 (Session Fixation) が可能」というものがありました。「セッション ID の固定化」を防止するには、ウェブアプリケーション (「XOOPS」など) を修正する方法と、それ以外[2]の部分で対処する方法があります。本届出は、製品開発者により脆弱性ではないと判断されましたが、「XOOPS」は、第三者がセッション ID を固定できないようプログラムが変更されましたので、ウェブサイトの管理者はアップデートしてください。

---

[1] 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。

[2] ウェブアプリケーション側で対処しない場合は、「Cookie Monster」と呼ばれるドメインをまたがった Cookie のセットができてしまう問題を抱えたブラウザ (Mozilla、Firefox などが該当) をそのウェブアプリケーションのログインに使用しないようにする必要があります。また、加えて、ウェブアプリケーションサーバ製品に「セッション ID の固定化」の脆弱性がある場合には、パッチを適用するか、設定で回避する必要があります。

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[3]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 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	28	117
②	海外 CSIRT から連絡を受けたもの	27	129
	計	55	246

(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 9 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 38%の届出が 45 日以内に公表されています。

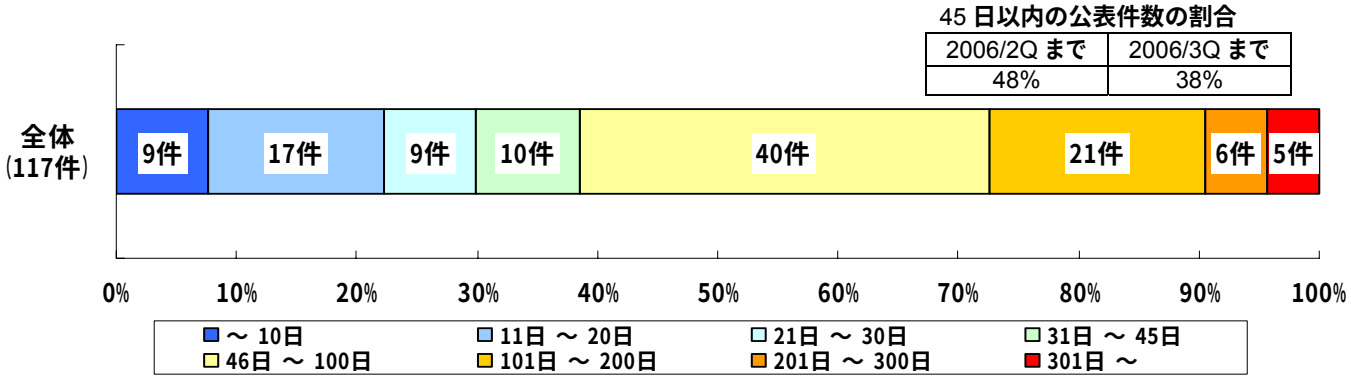


図 2-5 ソフトウエア製品の脆弱性 公表日数

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。

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、1 件 (項番 1) であり、特定の製品に関する脆弱性は 27 件でした。なお、19 件 (表 2-2 内の*1) 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。

表 2-2 2006 年第 3 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 (*1)	複数の Wiki クローン製品におけるサービス運用妨害 (DoS) の脆弱性	複数の Wiki クローン製品には、特定のリクエストを処理する際にサーバリソースを過剰に消費する問題があります。このため、サーバの処理速度が極端に低下し、サービス不能状態になる可能性があります。	2006 年 7 月 3 日

[3] 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
特定製品の脆弱性	2 (*1)	「ACollab」における SQL インジェクションの脆弱性	ウェブグループウェアシステム「ACollab」は、ユーザから入力された内容を元に SQL 文を組み立てる処理に問題があります。このため、第三者により任意の SQL 命令を実行される可能性があります。	2006 年 7 月 6 日
	3 (*1)	「ATutor」におけるクロスサイト・スクリプティングの脆弱性	e ラーニング用コンテンツ管理システム「ATutor」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 7 月 6 日
	4 (*1)	「Ruby」において、alias 機能の問題でセーフレベル 4 がサンドボックスとして機能しない脆弱性	オブジェクト指向スクリプト言語「Ruby」において、信頼できないプログラムによるファイルアクセスや OS コマンドの実行などを制限するための「セーフレベル」を回避できる脆弱性が確認されました。本来制限しているはずの操作が実行されてしまう可能性があります。	2006 年 7 月 11 日
	5 (*1)	「Ruby」において、特定メソッドの問題でセーフレベル 4 がサンドボックスとして機能しない脆弱性	オブジェクト指向スクリプト言語「Ruby」において、信頼できないプログラムによるファイルアクセスや OS コマンドの実行などを制限するための「セーフレベル」を回避できる脆弱性が確認されました。本来制限しているはずの操作が実行されてしまう可能性があります。	2006 年 7 月 11 日
	6	「ServerView」におけるクロスサイト・スクリプティングの脆弱性	サーバ監視ソフトウエア「ServerView」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。	2006 年 7 月 12 日
	7	「ServerView」におけるディレクトリ・トラバーサルの脆弱性	サーバ監視ソフトウエア「ServerView」には、ディレクトリ・トラバーサルによって、意図しないファイルを表示してしまう問題があります。ディレクトリ・トラバーサルによって、意図しないファイルを表示してしまう問題があります。	2006 年 7 月 12 日
	8 (*1)	「Geeklog」におけるクロスサイト・スクリプティングの脆弱性	ウェブコンテンツ構築・管理ソフト「Geeklog」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。	2006 年 7 月 18 日
	9	「Loudblog」におけるクロスサイト・スクリプティングの脆弱性	ポッドキャスト配信用ブログの作成ソフト「Loudblog」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。	2006 年 7 月 18 日
	10 (*1)	「QwikiWiki」におけるクロスサイト・スクリプティングの脆弱性	Wiki クローン「QwikiWiki」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。	2006 年 7 月 18 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	11 (*1)	「Dokeos」におけるクロスサイト・スクリプティングの脆弱性	e ラーニング用ウェブアプリソフト「Dokeos」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。	2006 年 7 月 31 日
	12 (*1)	「Pixelpost」におけるクロスサイト・スクリプティングの脆弱性	アルバムソフト「Pixelpost」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。	2006 年 7 月 31 日
	13	「桐」におけるディレクトリ・トラバーサルの脆弱性	日本語データベースシステム「桐」には、メール解析コマンドの添付ファイルの取り扱いが適切でないため、本来とは違うディレクトリにファイルを保存できてしまう、ディレクトリ・トラバーサルの問題があります。	2006 年 8 月 10 日
	14 (*1)	「04WebServer」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバソフトウエア「04WebServer」には、エラー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 8 月 14 日
	15 (*1)	「04WebServer」におけるディレクトリ・トラバーサルの脆弱性	ウェブサーバソフトウエア「04WebServer」には、ディレクトリ・トラバーサルによって、意図しないファイルを表示してしまう問題があります。	2006 年 8 月 14 日
	16 (*1)	「NetCommons」におけるクロスサイト・スクリプティングの脆弱性	e ラーニング用ウェブアプリソフト「NetCommons」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。	2006 年 8 月 14 日
	17 (*1)	「Owl」における SQL インジェクションの脆弱性	ドキュメント管理・公開システム「Owl」には、ユーザからの入力を取り扱う際の処理が不適切なため、任意の SQL コマンドを実行されてしまう、SQL インジェクションの問題があります。	2006 年 8 月 16 日
	18 (*1)	「Owl」におけるクロスサイト・スクリプティングの脆弱性	ドキュメント管理・公開システム「Owl」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。	2006 年 8 月 16 日
	19	「mail f/w system」においてメールの不正送信が可能な脆弱性	メール送信ソフト「mail f/w system」には、ヘッダ部分に相当する入力値に対する検査が不適切なため、管理者が設定していない宛先に電子メールを送信してしまう可能性があります。	2006 年 8 月 23 日
	20	「サイボウズ Office 6」における情報漏洩の脆弱性	ウェブベースのグループウェア「サイボウズ Office 6」には、登録されているユーザおよびグループに関する情報へのアクセス制限が不十分なため、これらの情報が漏えいしてしまう可能性があります。	2006 年 8 月 28 日
	21	複数のサイボウズ製品におけるディレクトリ・トラバーサルの脆弱性	サイボウズ社の複数のグループウェア製品には、ディレクトリ・トラバーサルによって、意図しないファイルを表示してしまう可能性があります。	2006 年 8 月 28 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	22 (*1)	「Webmin」および「Usermin」にクロスサイト・スクリプティングを含む複数の脆弱性	ウェブブラウザからシステムを管理する「Webmin」および「Usermin」には、ウェブページを出力する際の処理が不適切なため任意のスクリプトを埋め込まれる可能性があります。また、本来制限されているはずのファイルの実行や閲覧ができてしまう可能性があります。	2006 年 8 月 31 日
	23	Microsoft Windows の「インデックスサービス」におけるクロスサイト・スクリプティングの脆弱性	Microsoft Windows の「インデックスサービス」には、Internet Information Services(IIS)と組み合わせて検索機能を利用した場合に、第三者によりウェブページに任意のスクリプトを埋めこめてしまう、クロスサイト・スクリプティングの問題があります。	2006 年 9 月 13 日
	24 (*1)	「MDPro」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「MDPro」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。	2006 年 9 月 21 日
	25 (*1)	「SugarCRM」におけるクロスサイト・スクリプティングの脆弱性	オープンソースの顧客管理システム「SugarCRM」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。	2006 年 9 月 26 日
	26	「Movable Type」の検索機能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」の検索機能には、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。	2006 年 9 月 26 日
	27 (*1) (*2)	「Joomla!」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「Joomla!」には、ウェブページを出力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 9 月 28 日
	28 (*1) (*2)	「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。	2006 年 9 月 28 日

(*1) オープンソースソフトウエアの脆弱性

(*2) 製品開発者により既知の脆弱性と判断されたが、対策情報を周知するため公表したもの

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 24 件、英国 NISCC (National Infrastructure Security Co-ordination Centre) から 3 件の合計 27 件の脆弱性関連情報の連絡を受けました。このほか、9 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	Juniper JUNOS において IPv6 パケット処理にメモリリークの脆弱性	注意喚起として掲載[4]
2	Microsoft PowerPoint に遠隔から任意のコードが実行可能な脆弱性	注意喚起として掲載
3	Apache httpd の mod_rewrite モジュ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
4	Microsoft Windows の Server サービス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
5	MIT Kerberos5 (krb5)の krshd および v4rcp の権限昇格に関する脆弱性	複数製品開発者へ通知
6	Intel Centrino ワイヤレスネットワークドライバのフレーム処理に脆弱性	複数製品開発者へ通知
7	MIT Kerberos5 (krb5)の ftpd および ksu の権限昇格に関する脆弱性	複数製品開発者へ通知
8	Sony VAIO Media のメディアサーバ機能における遠隔から攻撃可能なバッファオーバフローの脆弱性	特定製品開発者へ通知
9	Sony VAIO Media のメディアサーバコンポーネントにおける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
10	Sony VAIO Media のメディアサーバコンポーネントにおけるディレクトリトラバーサルの脆弱性	特定製品開発者へ通知
11	Sony VAIO Media のメディアサーバ機能におけるバッファオーバフローの脆弱性	特定製品開発者へ通知
12	Sony SonicStage Mastering Studio における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
13	Intel 2100 PRO ワイヤレスネットワークドライバにおけるメモリ破損の脆弱性	複数製品開発者へ通知
14	BIND において複数の再帰問合せ処理時に INSIST エラーが発生する脆弱性	複数製品開発者へ通知
15	BIND の署名レコード問合せ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
16	複数の RSA 実装において署名が正しく検証されない脆弱性	注意喚起として掲載
17	Microsoft DirectAnimation パス ActiveX コントロールにおける入力値未チェックの脆弱性	注意喚起として掲載
18	gzip の make_table() の配列処理における脆弱性	複数製品開発者へ通知
19	gzip の LZH の取扱におけるバッファオーバーフローの脆弱性	複数製品開発者へ通知
20	gzip の LZH の取扱いにおいて無限ループが引き起こされる脆弱性	複数製品開発者へ通知
21	gzip におけるバッファオーバーフローの脆弱性	複数製品開発者へ通知
22	gzip の huft_build() における NULL ポインタ参照の脆弱性	複数製品開発者へ通知
23	OpenSSL の SSLv2 クライアントコードに NULL データをチェックできない脆弱性	複数製品開発者へ通知
24	OpenSSL の SSL_get_shared_ciphers()にバッファオーバフローの脆弱性	複数製品開発者へ通知

[4] 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。

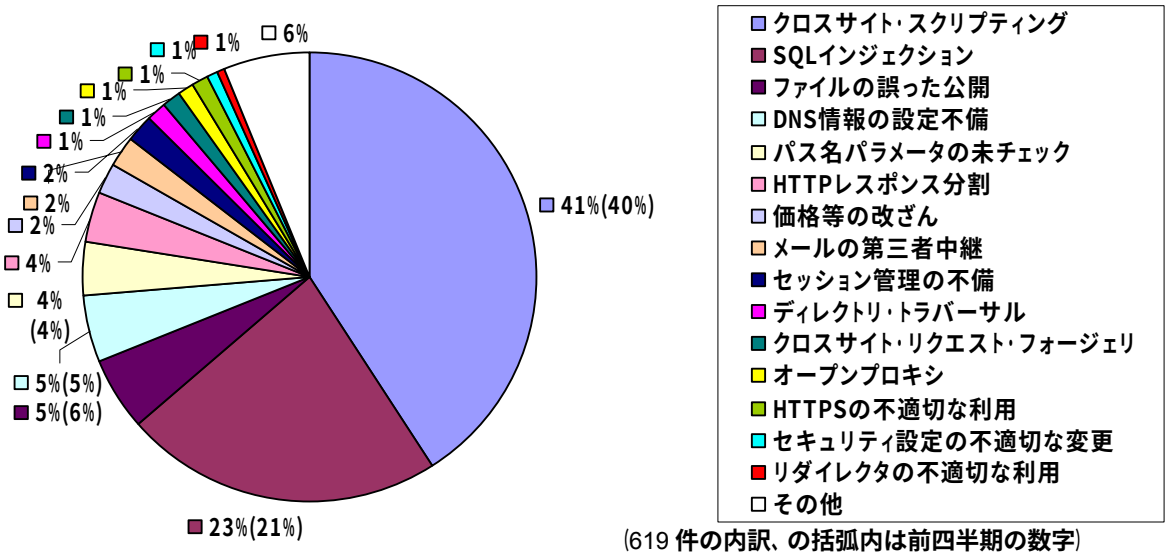
表 2-4 NISCC から連絡を受けた脆弱性関連情報および対応状況

項番	脆弱性	対応状況
1	HP OpenView Storage Data Protector の脆弱性	特定製品開発者へ通知
2	BIND 9 ソフトウエアに複数のサービス運用妨害(DoS)の脆弱性	複数製品開発者へ通知
3	X.509 証明書の検証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

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 661 件のうち、不受理のものを除いた 619 件について、種類別内訳を図 3-1 に、種類別の届出件数の推移を図 3-2 に、脅威別内訳を図 3-3 に示します。



(619 件の内訳、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 9 月末まで) [1]

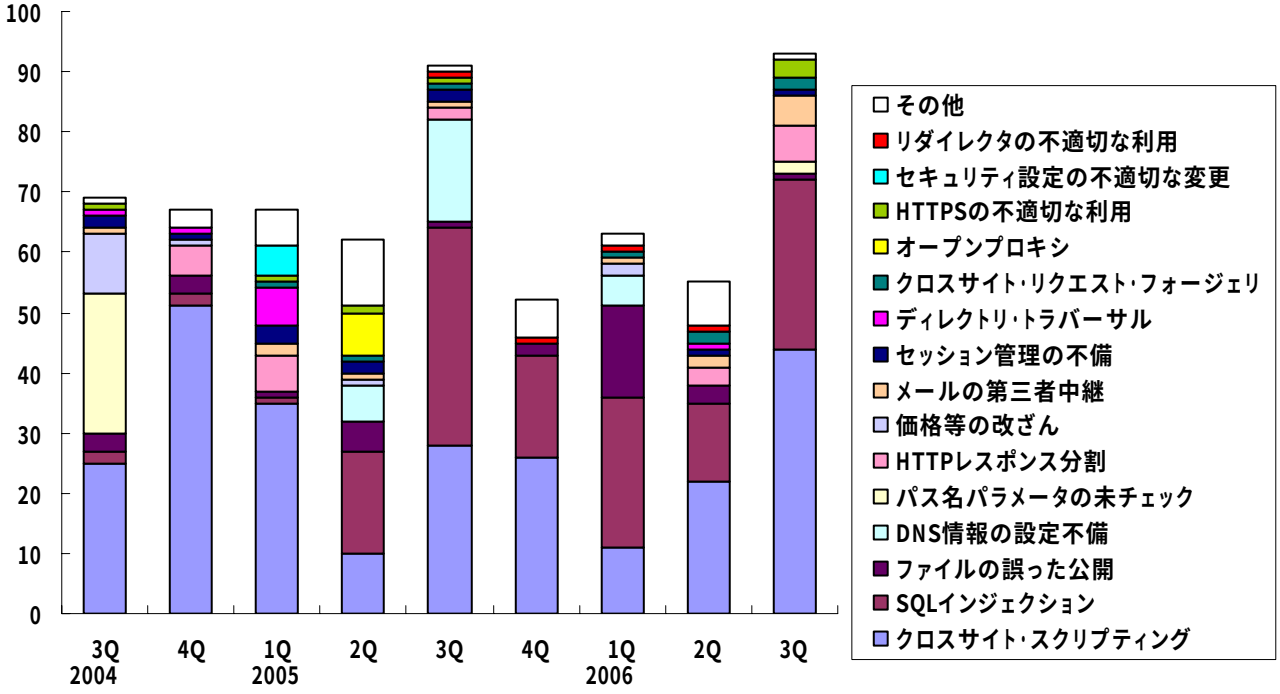
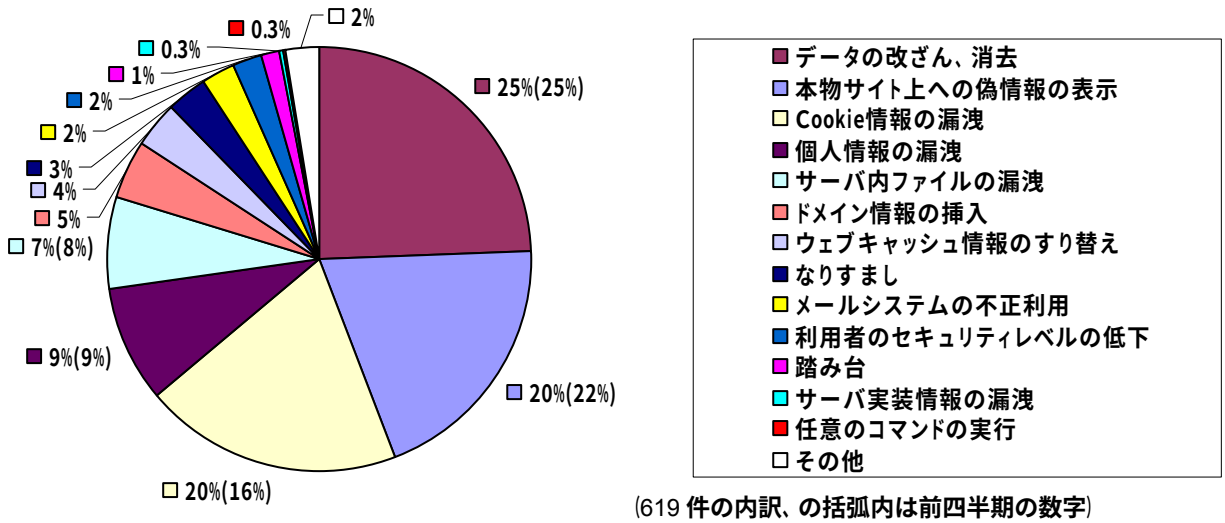


図 3-2 ウェブアプリケーションの脆弱性種類別件数の推移 (届出受付開始から 2006 年 9 月末まで) [1]



(619 件の内訳、の括弧内は前四半期の数字)

図 3-3　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 9 月末まで)

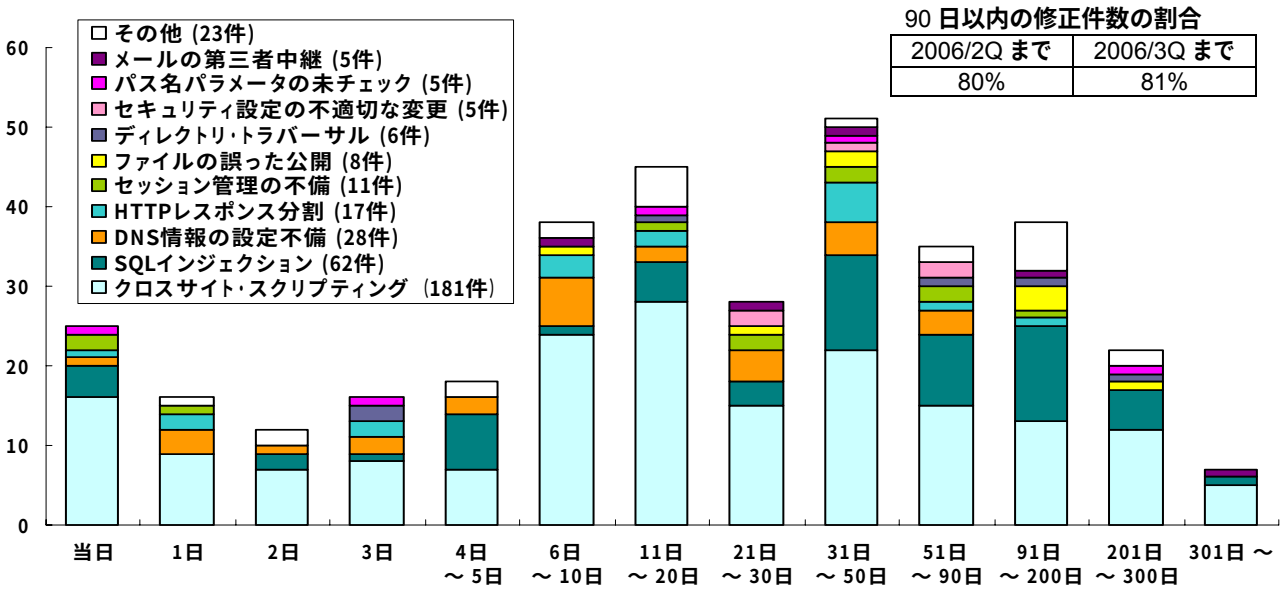
図 3-1 に示すように、脆弱性の種類は、「クロスサイト・スクリプティング」、「SQL インジェクション」が多くあります。

図 3-2 に示すように、「クロスサイト・スクリプティング」は届出開始当初から多く届出があります。「SQL インジェクション」の届出は 2005 年第 2 四半期から急増していますが、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 97 件のうち、問題が実際にあり修正したとの報告を受けたものは 6 割であり、残りの 4 割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。

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「本物サイト上への偽情報の表示」「Cookie 情報の漏洩」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 9 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 5 割の届出が 30 日以内、全体の 8 割の届出が 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

2006/2Q まで	2006/3Q まで
80%	81%

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

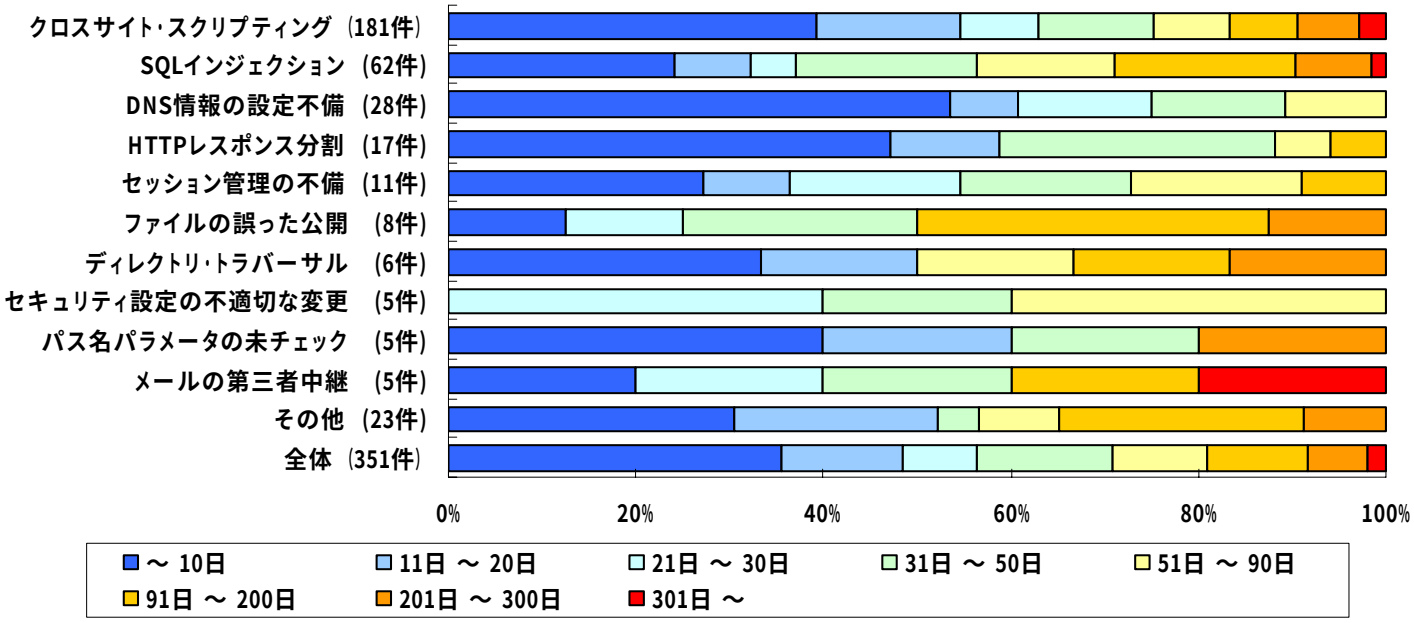


図 3-5　ウェブアプリケーションの脆弱性修正に要した日数の傾向

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。

参考 1

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

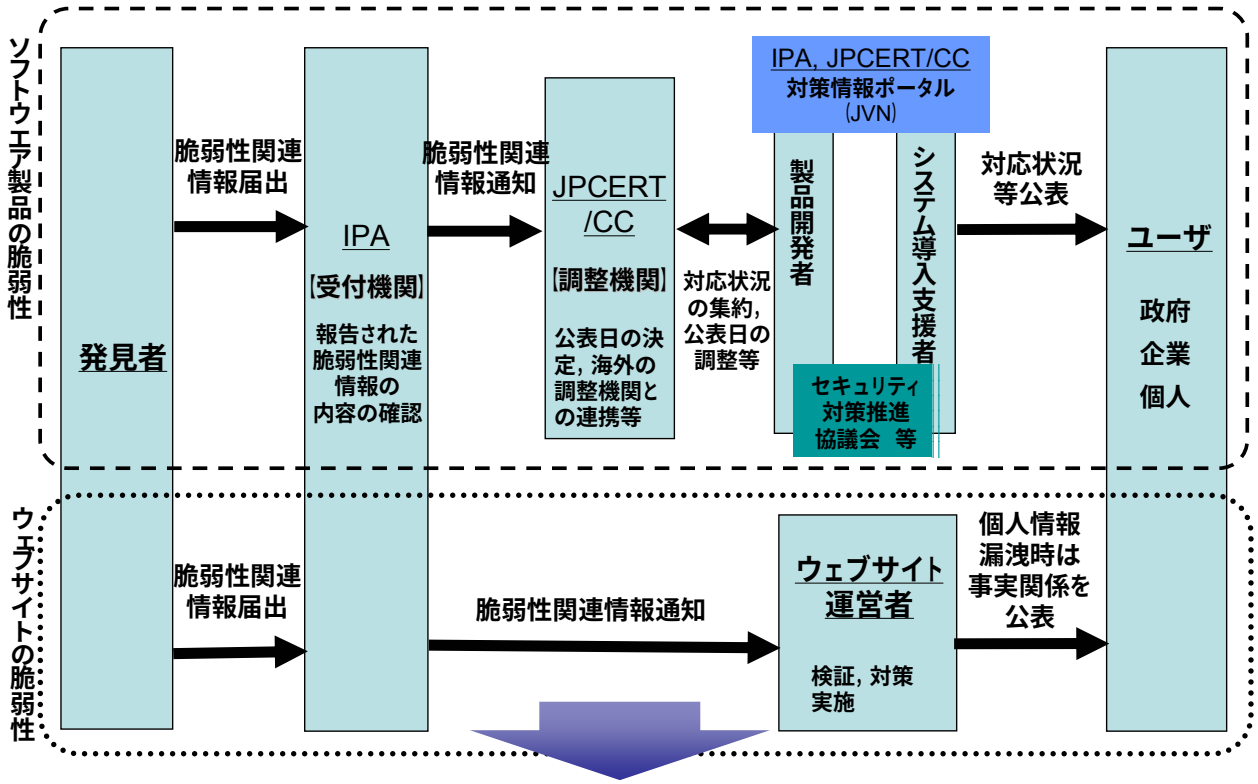
	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
3	ディレクトリ・トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	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	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
14	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
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

参考 2

「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