プレスリリース
2007年1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

ソフトウェア等の脆弱性関連情報に関する届出状況[2006年第4四半期(10月～12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、今般、2006年第4四半期(10月～12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ェア製品の脆弱性関連情報
・届出　　:122件(届出受付開始からの累計は416件)
・脆弱性公表:25件(届出受付開始からの累計は142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　　:89件(届出受付開始からの累計は750件)
・修正完了　:52件(届出受付開始からの累計は403件)

2. 今四半期の特徴

今四半期は、ソフトウェア製品に関するもの122件、ウェブサイトに関するもの89件、合計211件の届出があり、ソフトウェア製品に関する届出件数が過去最高を記録しました。

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6ヶ月が経過し、ソフトウェア製品に関するもの累計416件、ウェブサイトに関するもの累計750件、合計1,166件の届出があり、今四半期で1,000件を突破しました(図1)。

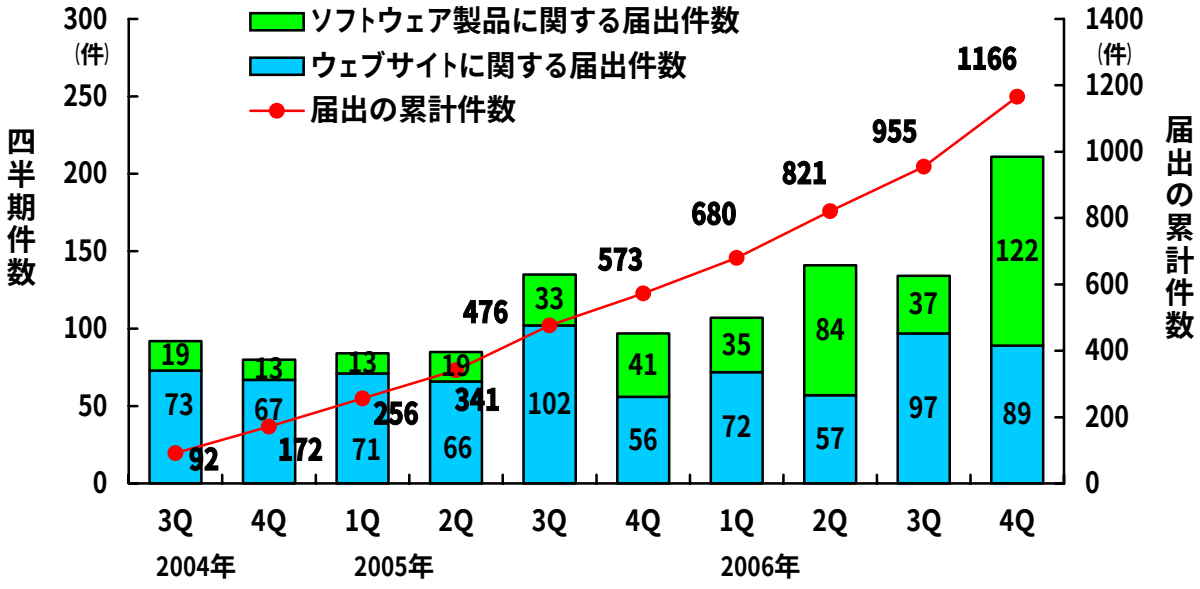


図1. 脆弱性の届出件数の四半期別推移

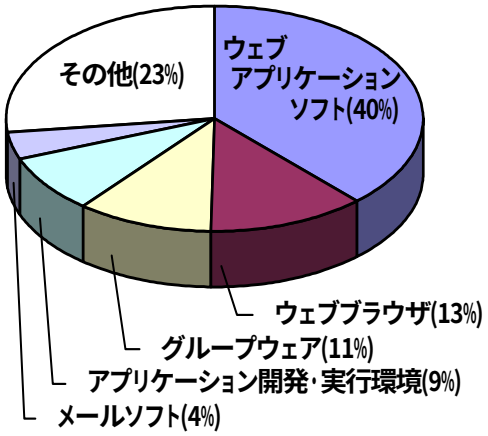
また、ソフトウェア製品に関して脆弱性の対策状況を25件公表しました。この中には、オープンソースソフトウェアに関するものが15件、組込みソフトウェアに関するものが3件ありました。なお、製品開発者自身から自社製品に関する脆弱性対策情報について連絡をうけ公表したものが3件ありました。

ウェブサイトに関してはウェブサイト運営者により脆弱性が修正されたものが52件ありました。このうち9件はIPAが修正を確認しました。

3. ソフトウェア製品の脆弱性の内訳

今四半期に届出が多かったソフトウェア製品について、届出累計416件のうち不受理67件を除いた349件の製品種類別内訳は、ウェブアプリケーションソフトが40%、ウェブブラウザが13%、グループウェアが11%、アプリケーション開発・実行環境が9%、メールソフトが4%などとなっています（図2）。

発見者が届出時に想定した脅威別の内訳の推移は図3のようになっており、今四半期の届出122件のうち不受理14件を除いた108件の内訳は、任意のスクリプトの実行[1]が69件、なりすましが8件、情報の漏えいが8件、任意のコードの実行が4件などで、任意のスクリプトの実行が特に増加しています（図3）。



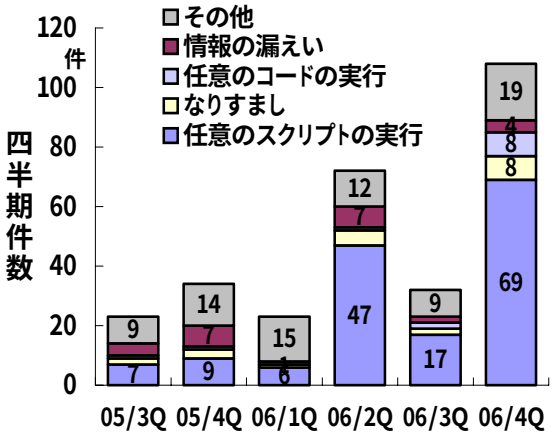


図2. ソフトウェア製品の脆弱性の製品種類別内訳　図3. ソフトウェア製品の脆弱性の脅威別内訳推移

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　改訂第2版」を2006年11月1日に公表しました。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。

「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

■ソフトウェア等の脆弱性関連情報に関する届出制度について

経済産業省告示に基づき、2004年7月より開始したものです。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。

■ 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

[1] 任意のスクリプトの実行：攻撃者が意図して作成したスクリプトが実行される脅威。スクリプトは、JavascriptやVBScriptなどで記述され、利用者のウェブブラウザ上で実行される。

別紙1

1. 届出状況

2006 年 10 月 1 日から 12 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 122 件、ウェブアプリケーション（ウェブサイト）に関するもの 89 件、合計 211 件であり、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 416 件、ウェブアプリケーション（ウェブサイト）に関するもの 750 件、合計 1,166 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 1.92 件であり、前四半期より増加しています。

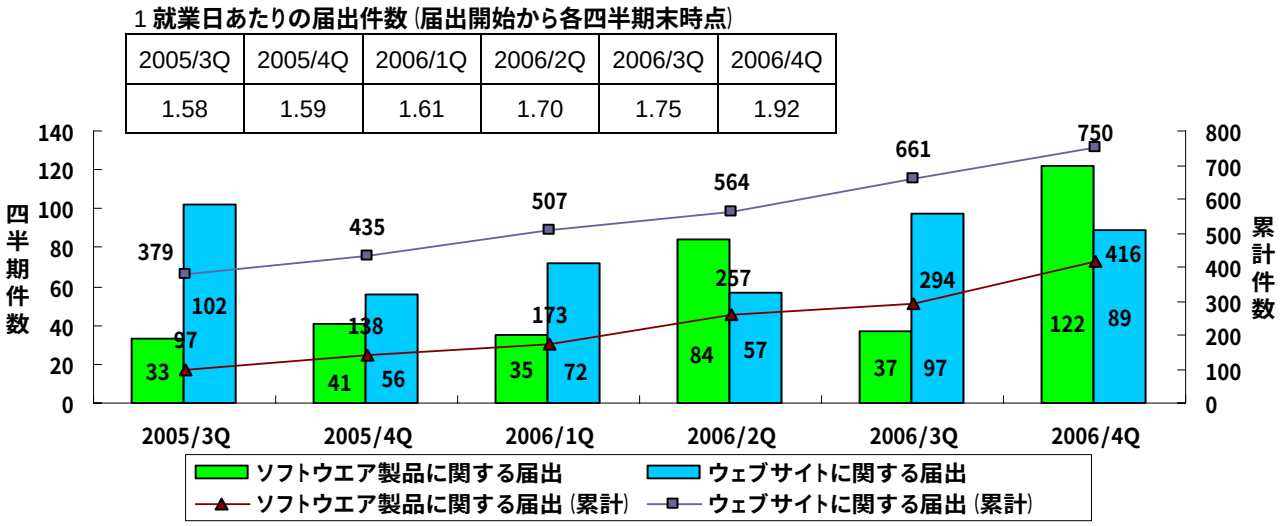
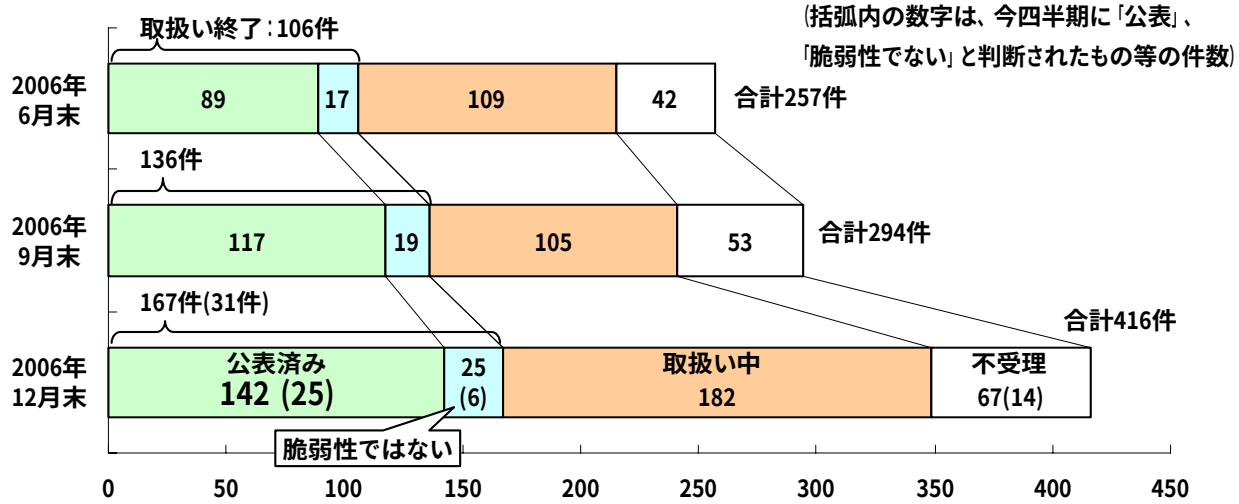


図 1-1 脆弱性関連情報の四半期別届出件数の推移

(1) ソフトウェア製品の脆弱性

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 1-2 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、25 件（累計 142 件）です。また、「不受理」としたものは 14 件（累計 67 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

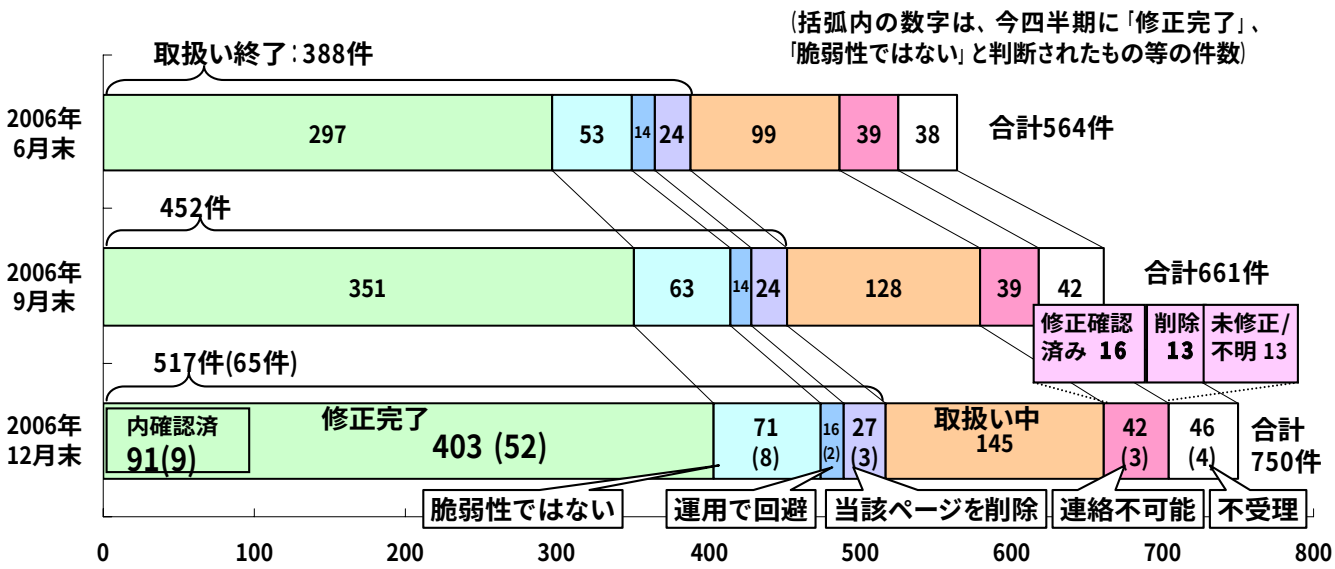
図 1-2 ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

⑵ ウェブサイトの脆弱性

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 1-3 に示します。

図 1-3 に示すとおり、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 65 件（累計 517 件）でした。このうち、「修正完了」したものは 52 件（累計 403 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 8 件（累計 71 件）ありました。「修正完了」したもののうちの 9 件（累計 91 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 46 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、13 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. 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

2.1 ソフトウェア製品の脆弱性情報

図 2-1 に、2005/Q2 から今四半期までに IPA に届出られたソフトウェア製品の内訳を示します。今四半期はオープンソースソフトウェア（OSS）以外のソフトウェア製品の届出が特に増加しており 86 件ありました。これまでの四半期に比べ 3～5 倍の件数です。また、今四半期も OSS に関する届出が 36 件ありました。

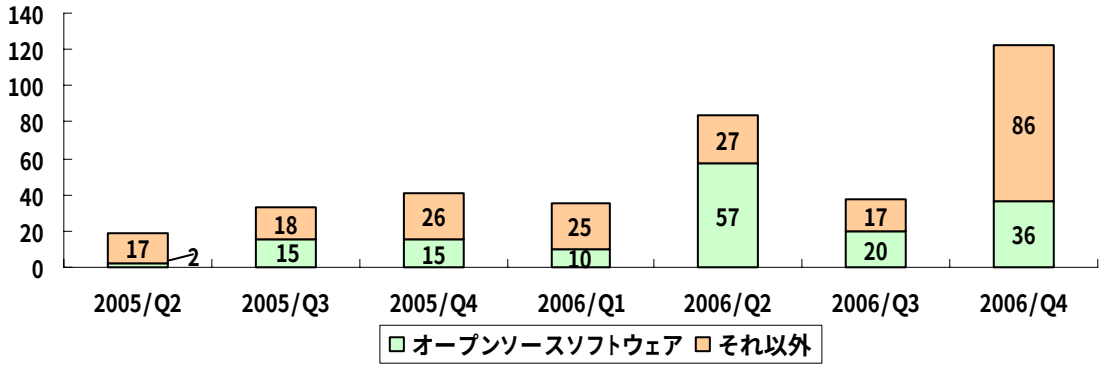
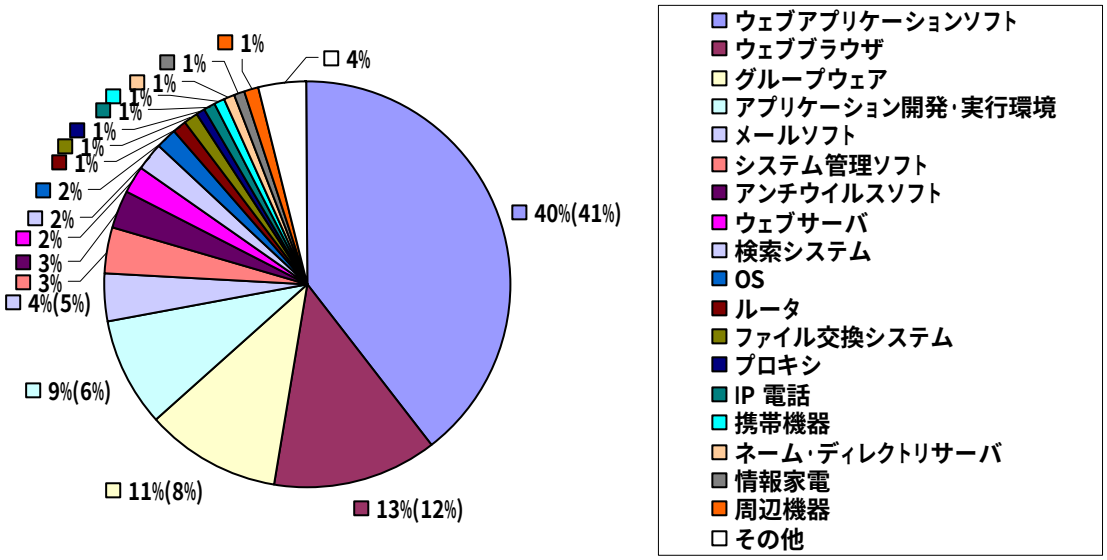


図 2-1 ソフトウェア製品の脆弱性 内訳（届出受付開始から 2006 年 12 月末まで）

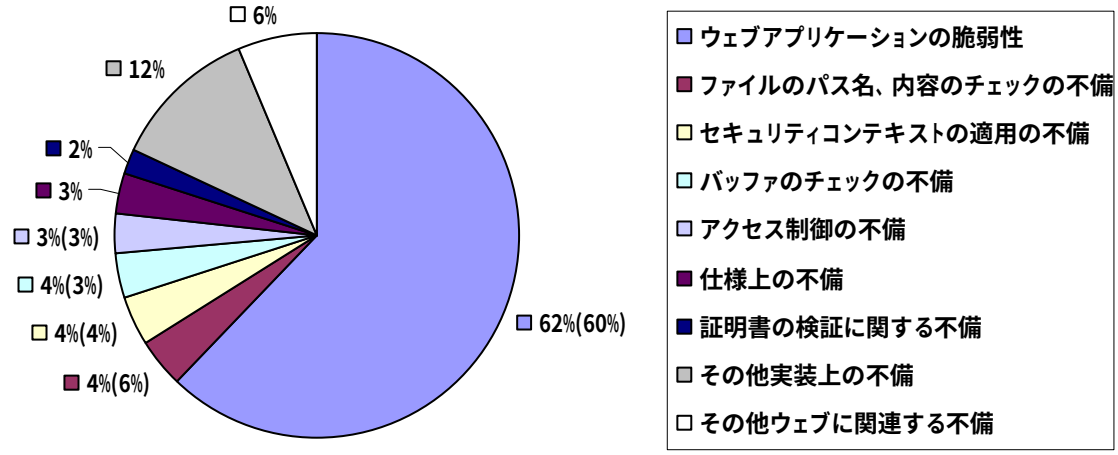
届出受付開始から今四半期までに IPA に届出られたソフトウェア製品に関する脆弱性関連情報 416 件のうち、不受理のものを除いた 349 件の製品種類別の内訳を図 2-2 に、原因別の内訳を図 2-3 に、脅威別の内訳を図 2-4 に示します。



※ その他には、データベース、ワープロソフト等があります （349 件の内訳、グラフの括弧内は前四半期の数字）

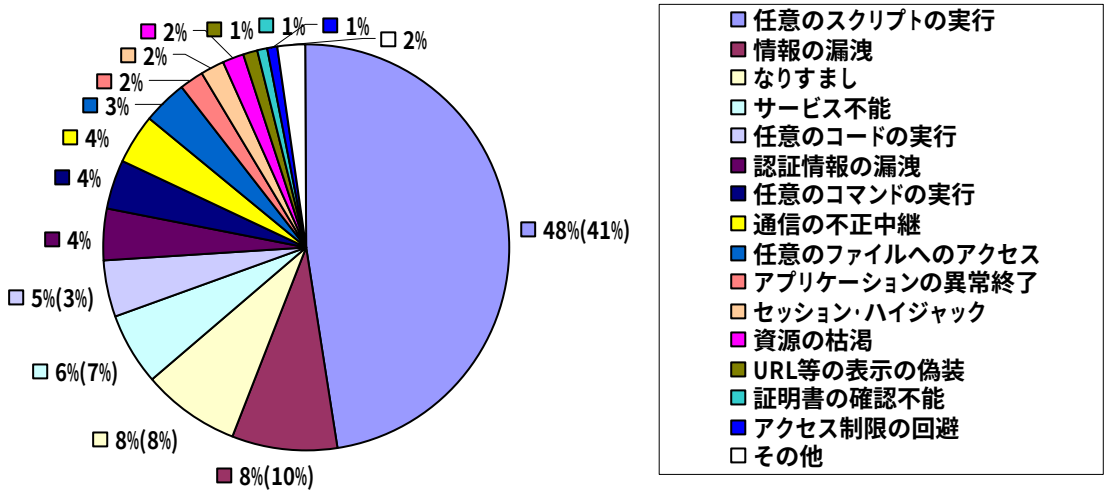
図 2-2 ソフトウェア製品の脆弱性 製品種類別内訳（届出受付開始から 2006 年 12 月末まで）

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。



(349 件の内訳、グラフの括弧内は前四半期の数字)

図 2-3 ソフトウェア製品の脆弱性 原因別内訳(届出受付開始から 2006 年 12 月末まで)[2]



(349 件の内訳、グラフの括弧内は前四半期の数字)

図 2-4 ソフトウェア製品の脆弱性 脅威別内訳(届出受付開始から 2006 年 12 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。

2.2 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 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/)。

[2] それぞれの脆弱性の詳しい説明については付表を参照してください。
[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。

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	25	142
②	海外 CSIRT から連絡を受けたもの	12	141
	計	37	283

(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 12 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 41%の届出が 45 日以内に公表されています。

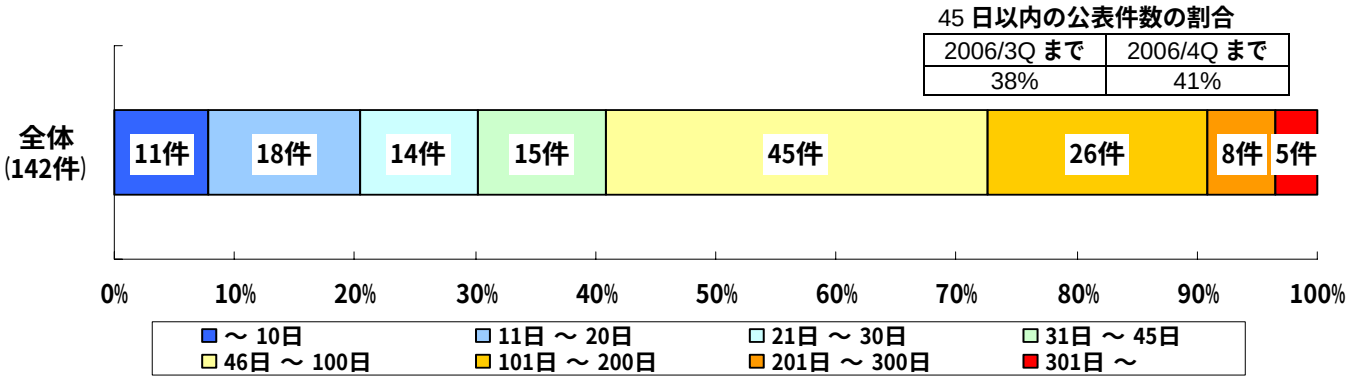


図 2-5 ソフトウェア製品の脆弱性 公表日数

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、「『一太郎』におけるバッファオーバーフローの脆弱性」(表 2-2 項番 3) や「『花子』におけるバッファオーバーフローの脆弱性」(表 2-2 項番 19) を公表しました。両製品共に国内の利用者が多く、ウイルスやワーム、ボットといった攻撃手法で利用されやすい脆弱性に関するものです。

また、「『TeraStation HD-HTGL シリーズ』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」(表 2-2 項番 1) のように、管理者の利用する画面において脆弱性が残っている事例が引き続き見受けられます。利用者への公開部分に対する脆弱性対策はしっかり行なっている製品でも、管理画面アクセスへの配慮が不十分なことがあります。公開部分同様にセキュリティ対策を施してください。

今四半期は、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の公表は無く、特定製品に関する脆弱性を 25 件公表しました。なお、オープンソースソフトウェア製品に関するものが 15 件 (表 2-2 の(*1))、組込みソフトウェアに関するものが 3 件 (表 2-2 の(*2))、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うけ公表したものが 3 件 (表 2-2 の(*3)) ありました。

表 2-2 2006 年第 4 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
特定製品の脆弱性(*4)	1 (*2)	「TeraStation HD-HTGL シリーズ」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	バッファロー製 LAN 接続 ハードディスク「TeraStation HD-HTGL シリーズ」Web 設定画面において、脆弱性が確認されました。Web 設定画面にログインした状態で悪意あるページよりリンクをたどった場合、ハードディスク上のデータが削除されたり、設定が変更される可能性があります。	2006 年 10 月 2 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(*4)	2	「Kmail CGI」における認証回避の脆弱性	携帯電話ウェブブラウザから、メールサーバのメールを読み書きできるようにするソフト「Kmail CGI」には、認証を回避される脆弱性が存在します。「Kmail CGI」の利用者になりすまされ、メールを読まれたり、削除されたりする可能性があります。また、遠隔の第三者により、管理者権限で「Kmail CGI」の機能を悪用される可能性があります。	2006 年 10 月 12 日
	3	「一太郎」におけるバッファオーバーフローの脆弱性	日本語ワープロソフト「一太郎」には、バッファオーバーフローの脆弱性が存在します。このため任意のコードを実行される可能性があります。	2006 年 10 月 18 日
	4 (*2) (*3)	「NEC MultiWriter 1700C/7500C 」の FTP サーバにおける脆弱性	NEC のプリンタ「NEC MultiWriter 1700C/7500C」には、内蔵の FTP サーバを、他の FTP サーバへの踏台として利用可能な問題があります。	2006 年 10 月 20 日
	5 (*2) (*3)	「NEC MultiWriter 1700C」の Web サーバに認証回避の脆弱性	NEC のプリンタ「NEC MultiWriter1700C」には、内蔵の Web サーバにおいて、認証されていないユーザによってシステムの設定が変更可能な問題があります。	2006 年 10 月 20 日
	6	「desknet's」におけるバッファオーバーフローの脆弱性	グループウェア「desknet's」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。	2006 年 10 月 24 日
	7 (*1)	「ハイパー日記システム」におけるクロスサイト・スクリプティングの脆弱性	ウェブ日記の作成支援ソフト「ハイパー日記システム」の日記編集機能 (webif) 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 11 月 6 日
	8	「MyODBC 日本語変換機能版」におけるサービス運用妨害 (DoS) の脆弱性	MySQL データベースへの接続を中継する ODBC ドライバ「MyODBC 日本語変換機能版」には、特定の文字列を含むレスポンス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 11 月 6 日
	9 (*1) (*3)	「Kahua」におけるログインセッション共有の脆弱性	アプリケーション開発・実行環境である「Kahua」には、異なるアプリケーション間でログインセッションが共有される問題があります。 このため第三者に、本来利用できる範囲を超えてアプリケーションを利用される可能性があります。	2006 年 11 月 10 日
	10 (*1)	「Nucleus」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「Nucleus」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 11 月 14 日
	11 (*1)	「EC-CUBE」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」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 11 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(*4)	12 (*1)	「eyeOS」におけるクロスサイト・スクリプティングの脆弱性	デスクトップ環境を提供するシステム「eyeOS」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 11 月 20 日
	13 (*1)	「phpComasy」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「phpComasy」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 11 月 24 日
	14 (*1)	「tDiary」におけるクロスサイト・スクリプティングの脆弱性	ウェブ日記の作成支援ソフト「tDiary」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 11 月 27 日
	15	「Blogn(ぶろぐん)」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「Blogn(ぶろぐん)」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 11 月 29 日
	16	「Chama Cargo」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機能を提供するソフト「Chama Cargo」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 11 月 30 日
	17 (*1)	「TikiWiki」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「TikiWiki」には、ウェブページを出力する際のフィルタリング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 12 月 4 日
	18 (*1)	「Ruby」の CGI ライブラリ cgi.rb におけるサービス運用妨害(DoS)の脆弱性	オブジェクト指向スクリプト言語「Ruby」に含まれる"cgi.rb"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 12 月 4 日
	19	「花子」におけるバッファオーバーフローの脆弱性	統合グラフィックソフトウェア「花子」には、バッファオーバーフローの脆弱性が存在します。このため任意のコードを実行される可能性があります。	2006 年 12 月 5 日
	20 (*1)	「しょぼしょぼ日記システム(sns)」におけるクロスサイト・スクリプティングの脆弱性	ウェブ日記の作成支援ソフト「しょぼしょぼ日記システム(sns)」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 12 月 8 日
	21 (*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 12 月 21 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(*4)	22 (*1)	「a-blog」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「a-blog」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 12 月 22 日
	23 (*1)	「pnamazu」におけるクロスサイト・スクリプティングの脆弱性	全文検索システム「Namazu」の perl 版プログラムである「pnamazu」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 12 月 25 日
	24 (*1)	「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 12 月 28 日
	25 (*1)	「tDiary」における任意の Ruby スクリプトを実行される脆弱性	ウェブ日記の作成支援ソフト「tDiary」には、設定画面において入力された内容を評価する処理に問題があります。このため、悪意あるページに誘導された場合、ウェブサーバ内の情報が漏洩したり、改竄される可能性があります。	2006 年 12 月 28 日

(*1)：オープンソースソフトウェア製品の脆弱性、　(*2)：組込みソフトウェアの脆弱性

(*3)：製品開発者自身から届出られた自社製品の脆弱性

(*4)：今四半期は、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はありませんでした。

⑵ 海外 CSIRT から連絡を受け公表した脆弱性

表 2-3、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 12 件の脆弱性関連情報の連絡を受けました。このほか、8 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

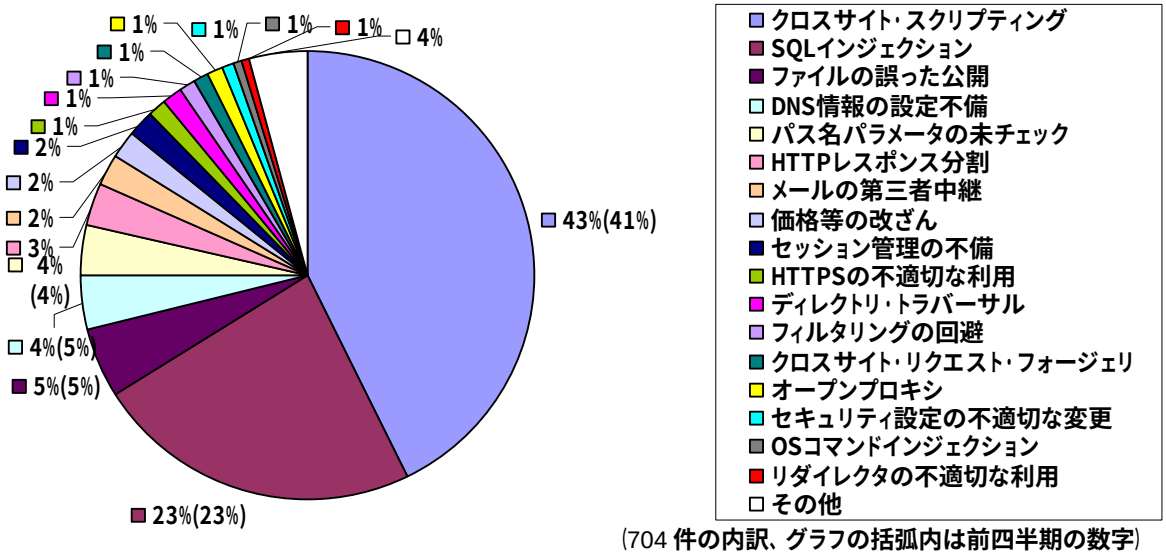
項番	脆弱性	対応状況
1	CruiseWorks にバッファオーバーフローの脆弱性	特定製品開発者へ通知
2	CruiseWorks にディレクトリトラバーサルの脆弱性	特定製品開発者へ通知
3	OpenSSH に SSH パケットの検証において多量のリソースを消費する脆弱性	特定製品開発者へ通知
4	OpenSSH におけるシグナルの扱いに関する脆弱性	特定製品開発者へ通知
5	Microsoft XMLHTTP ActiveX コントロールの脆弱性	注意喚起として掲載
6	Broadcom 無線 LAN デバイスドライバの 802.11 フレーム処理における脆弱性	特定製品開発者へ通知
7	Apple Mac OS X における DMG ファイルの取扱いに関する脆弱性	注意喚起として掲載
8	GNU gv 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	ImageKit 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	特定製品開発者へ通知

項番	脆弱性	対応状況
10	Microsoft Word の文字列処理に関する脆弱性	注意喚起として掲載
11	Intel ネットワークドライバにおける権限昇格の脆弱性	複数製品開発者へ通知
12	Yahoo Messenger の YMailAttach ActiveX コントロール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

3. ウェブサイトの脆弱性関連情報の取扱い

3.1 ウェブサイトの脆弱性情報

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サイトの脆弱性関連情報 750 件のうち、不受理のものを除いた 704 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。



(704 件の内訳、グラフの括弧内は前四半期の数字)

図 3-1 ウェブサイトの脆弱性種類別内訳 (届出受付開始から 2006 年 12 月末まで) [1]

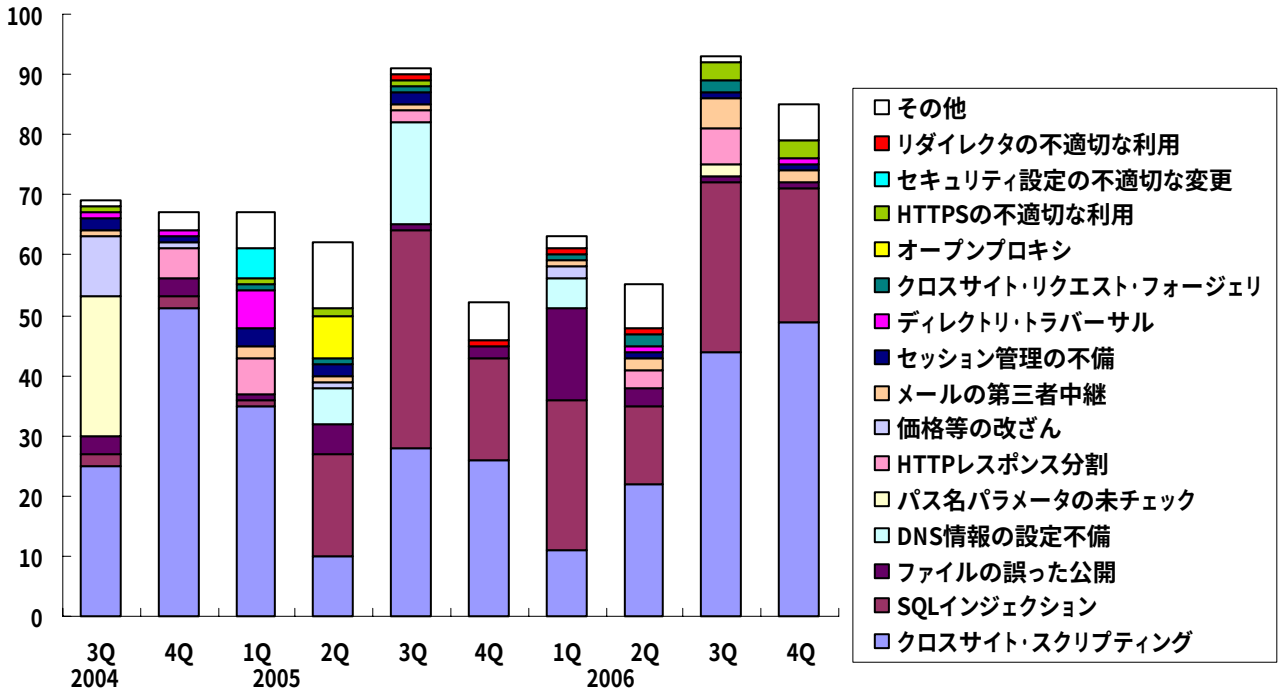
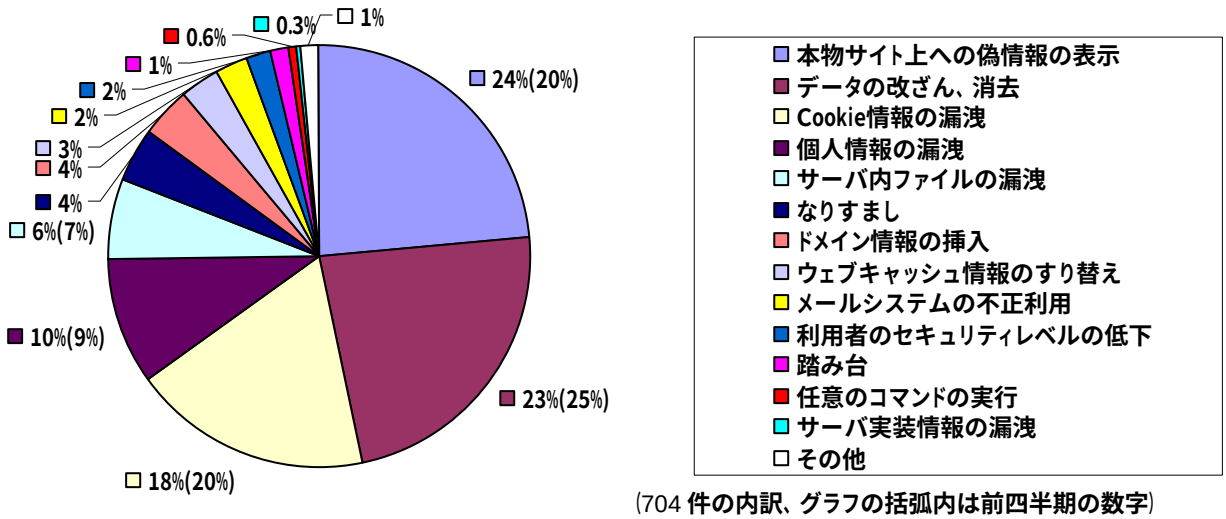


図 3-2 ウェブサイトの脆弱性種類別件数の推移 (届出受付開始から 2006 年 12 月末まで) [1]



(704 件の内訳、グラフの括弧内は前四半期の数字)

図 3-3　ウェブサイトの脆弱性脅威別内訳 (届出受付開始から 2006 年 12 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 3-2)、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 3-1)。

「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 3-3)。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。

3.2　ウェブサイトの脆弱性の修正状況

届出受付開始から 2006 年 12 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 3-4 および図 3-5 に示します。全体の 54%の届出が 30 日以内、全体の 80%の届出が 90 日以内に修正されています。

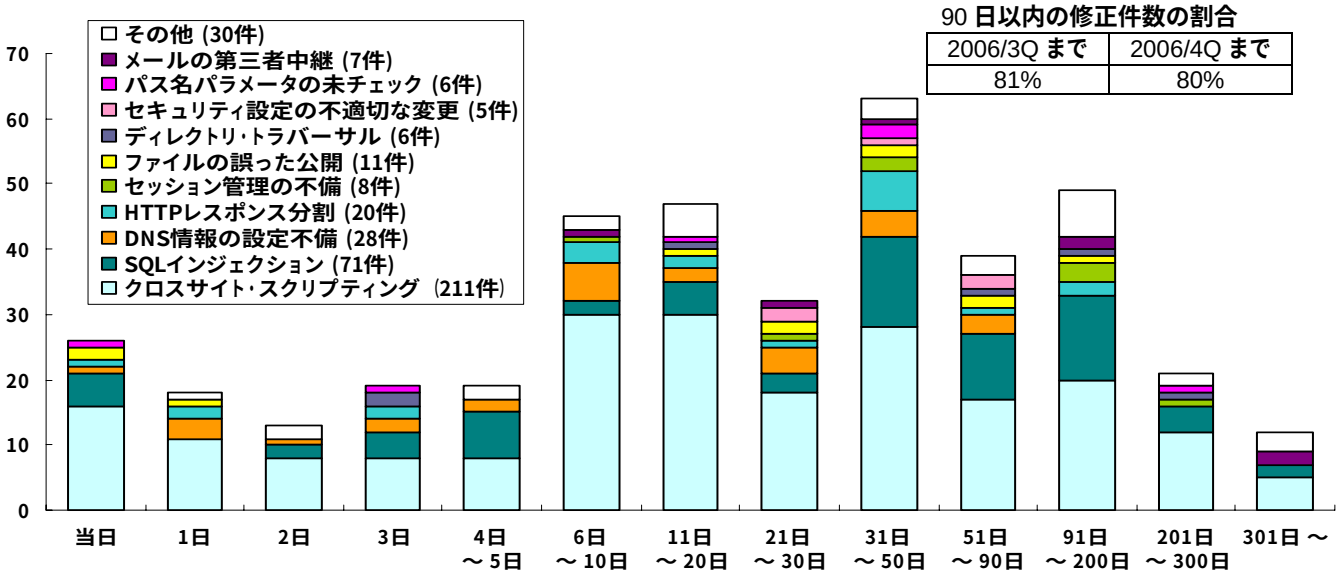


図 3-4　ウェブサイトの脆弱性修正に要した日数

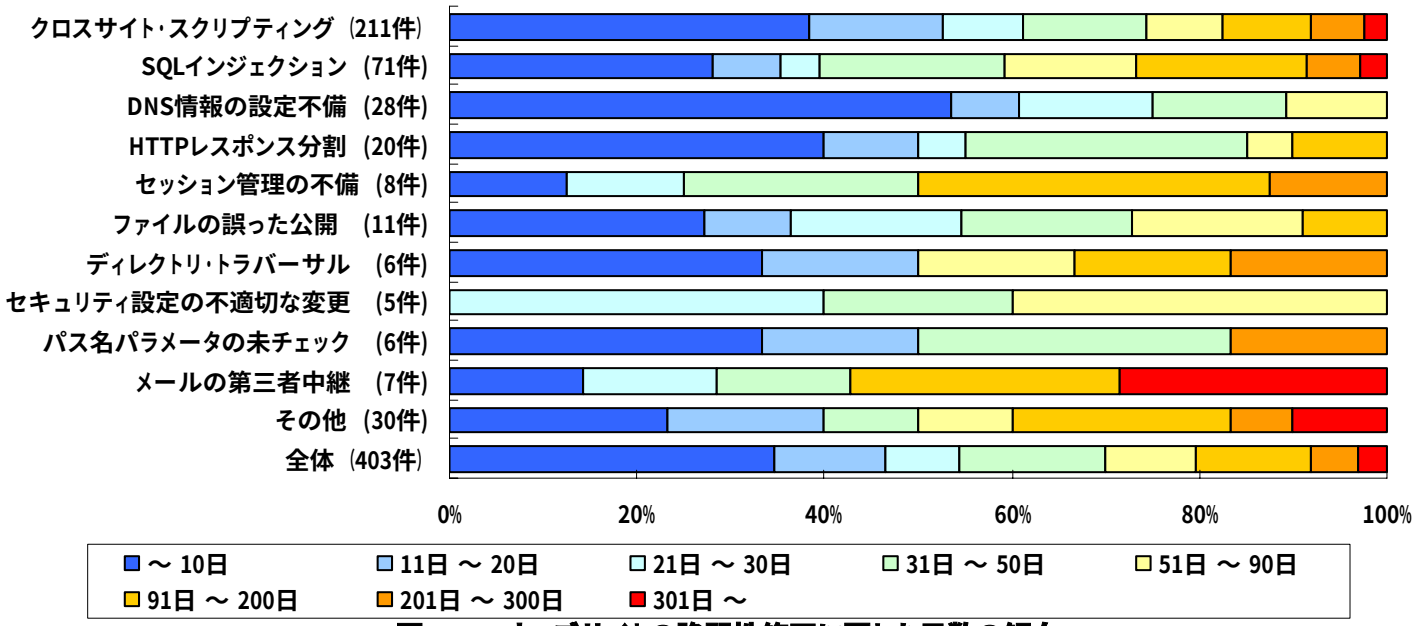


図 3-5　ウェブサイトの脆弱性修正に要した日数の傾向

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。

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。

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。

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

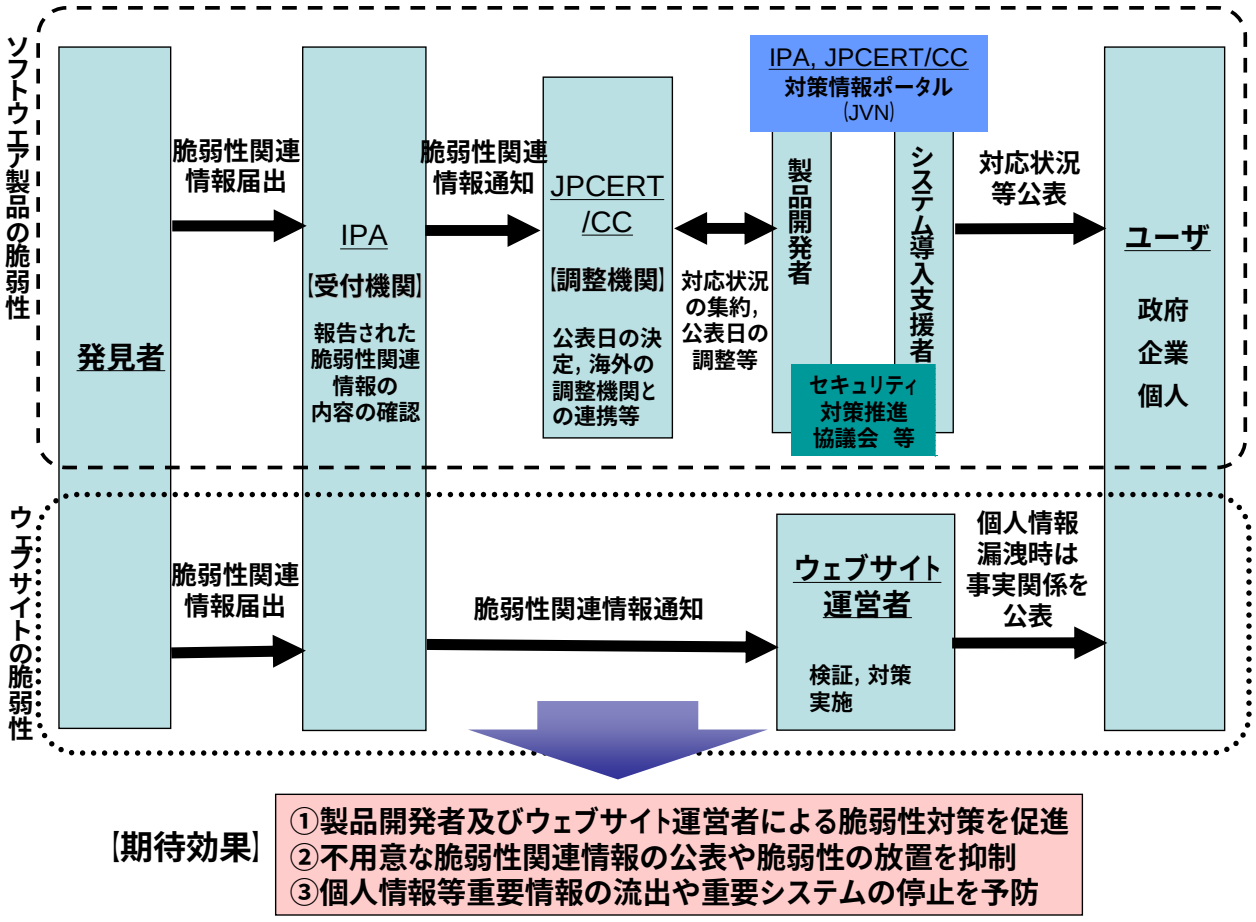
	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩

	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