プレスリリース
2006 年 1 月 16 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 [2005 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) 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「ソフトウエア等脆弱性関連情報取扱基準」(平成 16 年経済産業省告示 第 235 号) 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、2005 年第 4 四半期 (10 月～12 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

- ソフトウエア製品の脆弱性関連情報
  届出　　：39 件 (届出受付開始からの累計は 133 件)
  脆弱性公表：13 件 (届出受付開始からの累計は 54 件)
  なお、以上の他、製品開発者自身から脆弱性および対策情報の連絡を受けたものが 1 件ありました。
- ウェブアプリケーションの脆弱性関連情報
  届出　　：56 件 (届出受付開始からの累計は 435 件)
  修正完了　：57 件 (届出受付開始からの累計は 234 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脆弱性情報の届出において、オープンソースソフトウエアに関する届出が前期に引き続き 15 件あり、それ以前の件数を大きく上回っています(p.4 図 2-1 参照)。

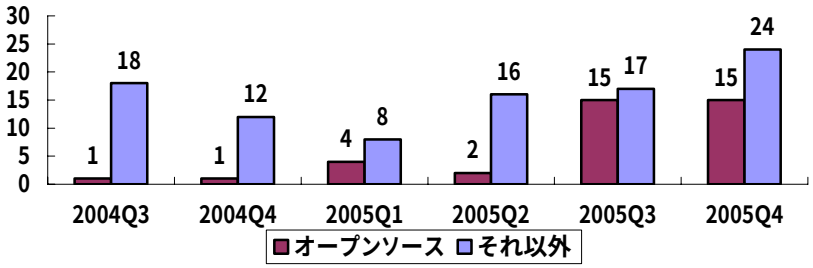


図　ソフトウエア製品の脆弱性 内訳 (届出受付開始から 2005 年 12 月末まで)

この間、JVN[1]で公表したものとして、組込み機器に関する届出である、≪携帯電話の Web ブラウザにおける Referer ヘッダの扱いに関する問題≫などがありました (p.8 表 2-2 項番 14 参照)。この他、前四半期に公表した≪「Tomcat」におけるリクエスト処理に関する脆弱性≫について、開発元である The Apache Software Foundation (ASF) から修正プログラムが提供されていない (2006 年 1 月 16 日現在) ため、IPA で本脆弱性を解消する修正プログラムを作成し公表しました (p.5 2.2 参照)。

[1] IPA および JPCERT/CC が対応状況ポータルサイト「JVN」を運営し、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]

2005 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、95 件（ソフトウエア製品に関するもの 39 件、ウェブアプリケーションに関するもの 56 件）であり、届出受付開始（2004 年 7 月 8 日）からの累計は 568 件（ソフトウエア製品に関するもの 133 件、ウェブアプリケーションに関するもの 435 件）です。四半期毎の届出状況を図 1-1 に示します。就業日 1 日当たりの届出件数は 1.58 件であり、前四半期より増加しています。

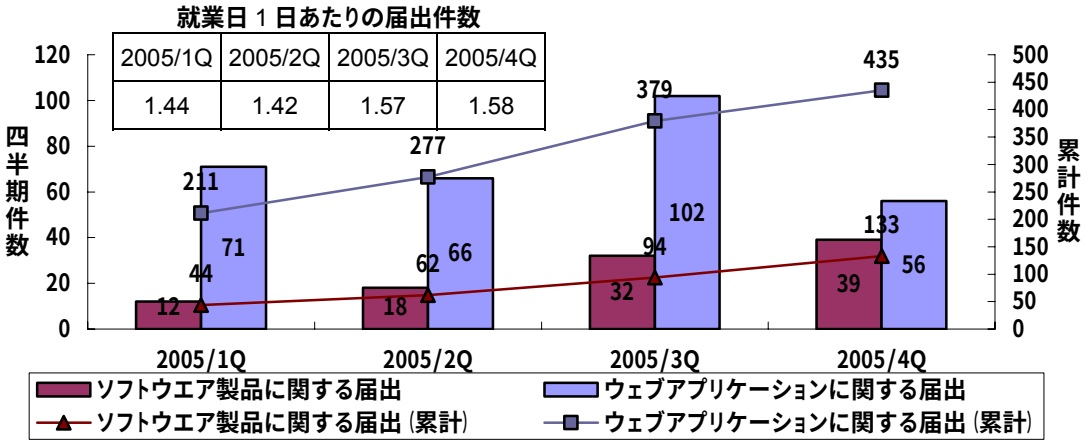
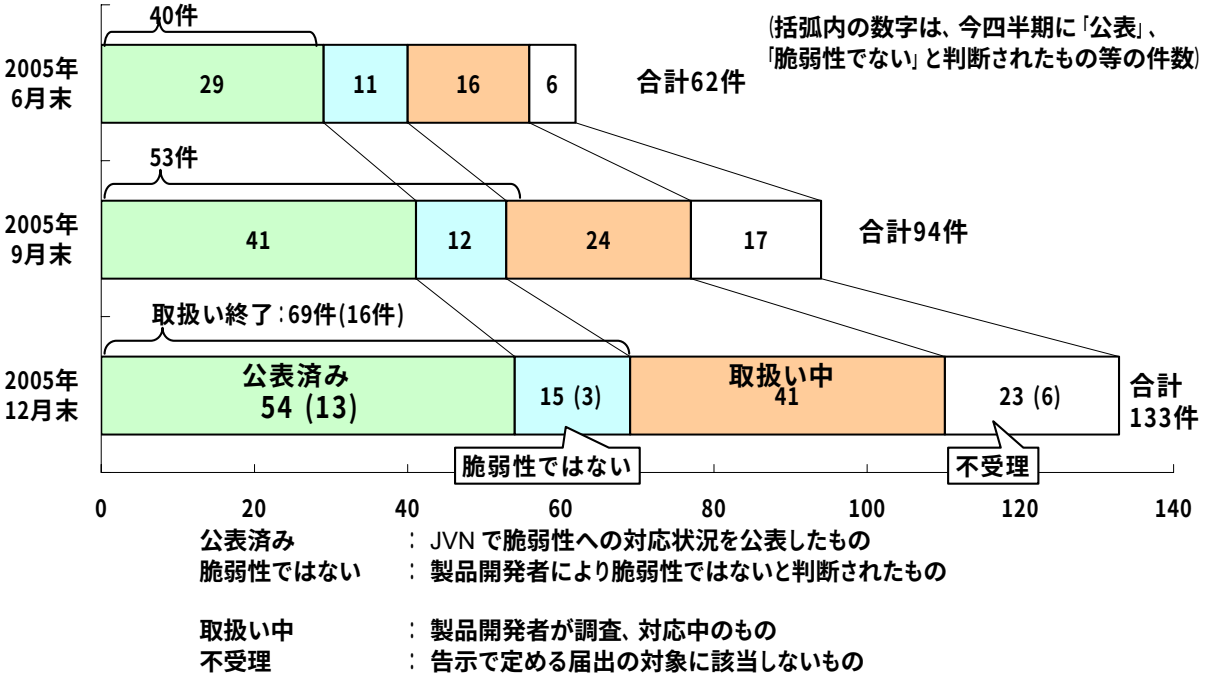


図 1-1 脆弱性関連情報の四半期別届出件数の推移

(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、13 件（累計 54 件）です。また、製品開発者により「脆弱性ではない」と判断されたものは 3 件（累計 15 件）、「不受理」としたものは 6 件（累計 23 件）ありました。「不受理」の届出についても、必要に応じて製品開発者に伝えています。



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] 届出件数は、実際にウェブフォームやメールで届出を受けた件数と同じではありません。1 つの届出に複数の脆弱性関連情報が含まれる場合は、その脆弱性の数だけ分割して計上しています。

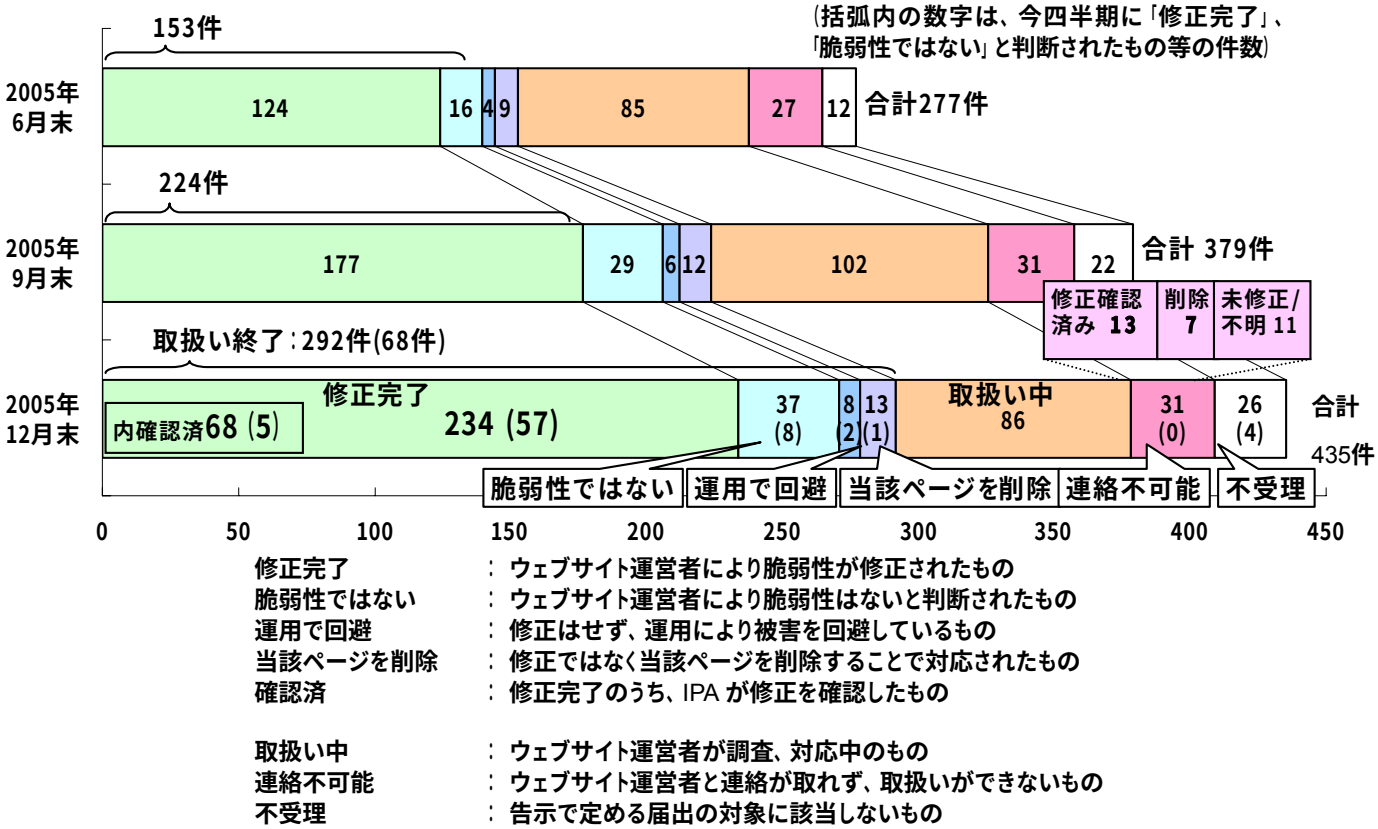
このほかに、製品開発者自身から脆弱性およびその対策情報の連絡を受け、公表したものが 1 件ありました。

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 68 件（累計 292 件）でした。このうち、「修正完了」したものは **57** 件（累計 **234** 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 37 件）、脆弱性を「運用で回避」すると対応されたものが 2 件（累計 8 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 1 件（累計 13 件）ありました。「修正完了」したものうちの 5 件（累計 68 件）はウェブサイト運営者からの依頼により IPA が修正を確認しました。

このほか、「不受理」としたものが 4 件（累計 26 件）ありました。「連絡不可能」の届出のうち、13 件は修正されています。その中には、ウェブサイト運営者とは連絡が取れ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、7 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と連絡が取れず、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。前四半期から、オープンソースソフトウエアに関する届出が増加しています。

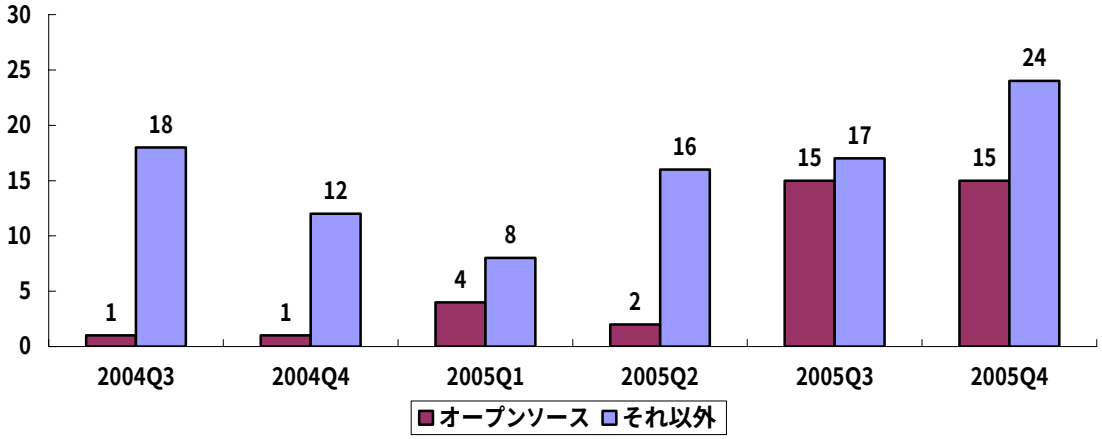
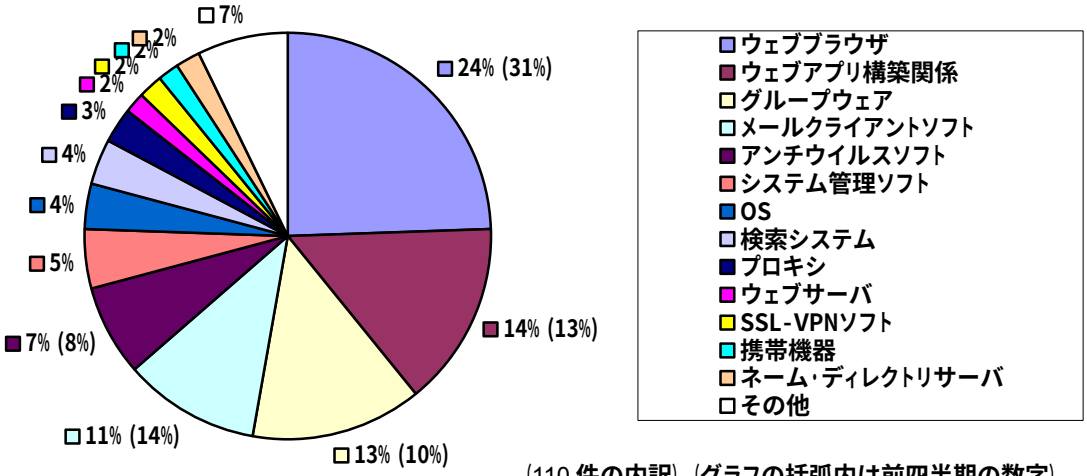


図 2-1　ソフトウエア製品の脆弱性 内訳（届出受付開始から 2005 年 12 月末まで）

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エア製品に関する脆弱性関連情報 133 件のうち、不受理のものを除いた 110 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。

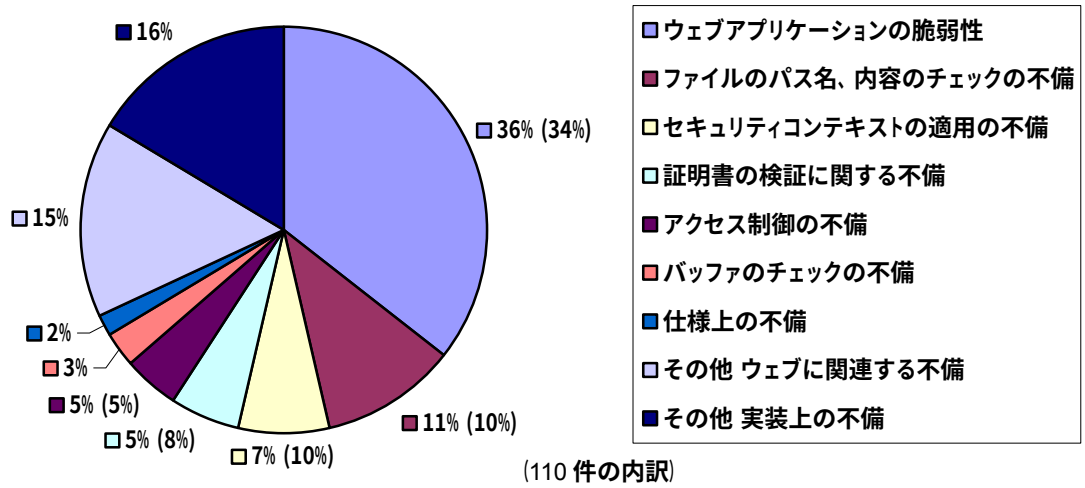


（110 件の内訳）（グラフの括弧内は前四半期の数字）

※1 件のものはその他に分類しています。
ウェブサーバ、プロキシサーバ、情報家電、ルータがあります

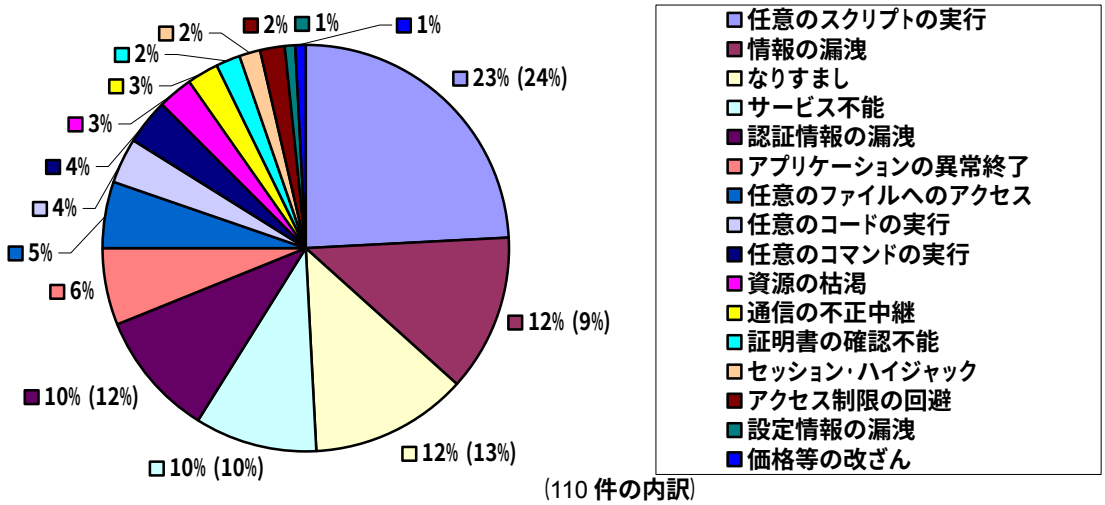
図 2-2　ソフトウエア製品の脆弱性 種類別内訳（届出受付開始から 2005 年 12 月末まで）

図 2-2 から、IPA に届出があった脆弱性には、「ウェブブラウザ」「ウェブアプリ構築関係」など、ウェブに関連する製品についての脆弱性が多くあります。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、情報家電や携帯機器などに関するものも含まれています。今四半期は、携帯電話によるインターネット接続サービスのブラウザにあった不具合について修正され、JVN で公表しました（後述）。



(110 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 2005 年 12 月末まで) [3]



(110 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 2005 年 12 月末まで)

図 2-3 から、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 から、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。

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 3 種類の脆弱性関連情報について、日本国内の製品開発者当の関係者、および海外 CSIRT[4]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/)。

また、前期に JVN で公表した≪「Tomcat」におけるリクエスト処理に関する脆弱性≫について、開発元である The Apache Software Foundation (ASF) から、正式な修正プログラムが提供されていない (2006 年 1 月 11 日現在) ため、IPA では、本脆弱性を解消する修正プログラムを作成し公表しました。

---

[3] 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。

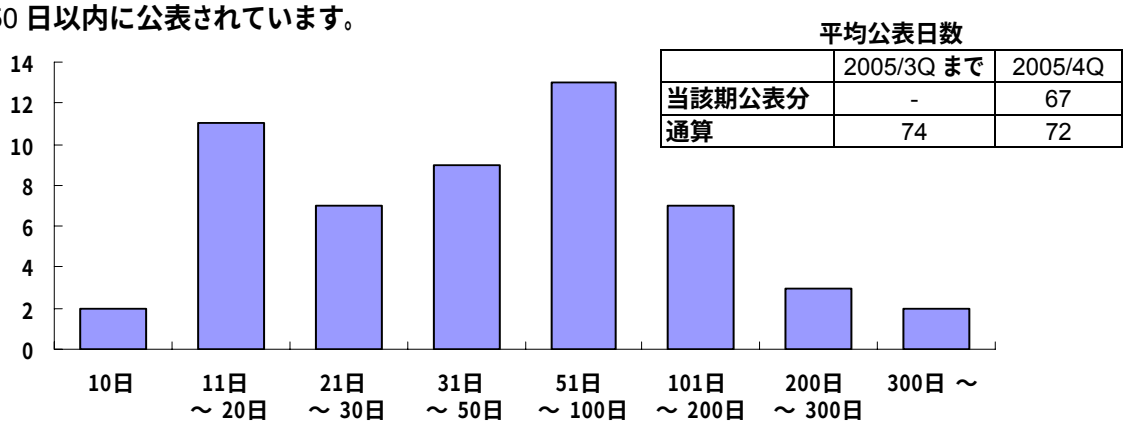
[4] CSIRT (Computer Security Incident Response Team) は、コンピュータセキュリティに関するインシデント (事故) への対応や調整、サポートをするチームのことです。

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 (1. (1) に記載)	13	54
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	1	5
③	海外 CSIRT から連絡を受けたもの	11	92
	計	25	151

(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 2005 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 54%の届出が 50 日以内に公表されています。



平均公表日数

	2005/3Q まで	2005/4Q
当該期公表分	-	67
通算	74	72

図 2-5 ソフトウエア製品の脆弱性 公表日数

表 2-2 に、国内の発見者および製品開発者から届出・連絡を受け、2005 年第 4 四半期に公表した脆弱性 (表 2-1 の①および②) 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、≪「OpenSSL」におけるバージョン・ロールバックの脆弱性≫ (表 2-3 項番 1)、≪「HTTPD-User-Manage」におけるクロスサイト・スクリプティングの脆弱性≫ (項番 2) の 2 件であり、特定の製品に関する脆弱性は 11 件でした。≪富士通製 Java Runtime Environment のリフレクション API に関する脆弱性≫ (項番 9) 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たものです (前述の②)。また、≪「携帯電話の Web ブラウザにおける Referer ヘッダの扱いに関する問題≫ (項番 14) は、製品開発者により脆弱性ではないとされていますが、ユーザへの周知を目的として、対策情報を JVN へ公開しました。

表 2-2 2005 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
複数開発者製品に影響がある脆弱性	1	「OpenSSL」におけるバージョン・ロールバックの脆弱性	ウェブサーバなどで SSL による暗号化通信を行うためのライブラリ「OpenSSL」に、利用するプロトコルのバージョンを低下させ、弱い暗号化通信方式を強制できてしまう問題があります。	2005 年 10 月 12 日
	2	「HTTPD-User-Manage」におけるクロスサイト・スクリプティングの脆弱性	ブラウザからウェブサーバのユーザ管理を行う「HTTPD-User-Manage」には、入力内容のエスケープ処理に漏れがあります。そのため、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。	2005 年 11 月 16 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	「eBASEweb」における SQL インジェクションの脆弱性	販売促進用商品情報のデータ管理ソフトウエア「eBASEweb」には、ユーザの入力から SQL クエリを作成する際のエスケープ処理に漏れがあります。そのため、第三者により任意の SQL 命令をデータベース上で実行される可能性があります。	2005 年 10 月 21 日
	4	「XOOPS」におけるクロスサイト・スクリプティングの脆弱性	ウェブコンテンツ管理システム「XOOPS」には、独自のタグコード XOOPS Code の検査処理及び、フォーラムモジュールにおける投稿表示に関する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。	2005 年 10 月 24 日
	5	「Hyper Estraier」におけるディレクトリ・トラバーサル/サービス不能の脆弱性	全文検索システム「Hyper Estraier」には、Unicode のファイル名を適切に取り扱わない問題があります。そのため検索用インデックスが作成できなかったり、検索対象外のファイルを検索用インデックスに登録してしまう可能性があります。	2005 年 10 月 28 日
	6	Kent Web 「PostMail」におけるメール第三者中継の脆弱性	ウェブフォームの入力内容をメール送信する「PostMail」には、細工された文字列が与えられると、あらかじめ決められた以外の宛先にメールを送信する問題があります。そのため、ウェブサイトが迷惑メールの踏み台になる可能性があります。	2005 年 11 月 11 日
	7	「FreeStyleWiki」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チェックが不十分な問題があります。そのため、第三者によりウェブコンテンツに任意のスクリプトが埋め込まれる可能性があります。	2005 年 12 月 5 日
	8	「MitakeSearch」におけるクロスサイト・スクリプティングの脆弱性	全文検索ソフトウエア「MitakeSearch」の検索度合いを評価するランキング表示に関するエスケープ処理に漏れがあります。そのため、第三者によりランキング機能の画面に任意のスクリプトが埋め込まれる可能性があります。	2005 年 12 月 5 日
	9	富士通製 Java Runtime Environment のリフレクション API に関する脆弱性	富士通製の Java Runtime Environment に含まれるリフレクション API には脆弱性があります。そのため、Java アプレットが、セキュリティ設定を無視して、許可されている以上の権限で実行される可能性があります。	2005 年 12 月 13 日
	10	「Opera」におけるブックマーク機能に関する脆弱性	「Opera」ウェブブラウザには、TITLE 要素に長い文字列を含むウェブページをブックマークに登録すると、「Opera」起動時にエラーが出て異常終了してしまい、起動できなくなる問題があります。	2005 年 12 月 14 日
	11	「mod_imap」におけるクロスサイト・スクリプティングの脆弱性	Apache HTTP Server のサーバサイドイメージマップ処理モジュール「mod_imagemap」「mod_imap」には、HTTP ヘッダの処理に問題があります。そのためイメージマップに任意のスクリプトが埋め込まれる可能性があります。	2005 年 12 月 15 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
	12	「WebNote Clip」における OS コマンド・インジェクションの脆弱性	伝言板などの記入式ホームページを作成する「WebNote Clip」には、リクエスト内容の確認が不十分な問題があります。そのため、サーバ上で OS コマンドを実行される可能性があります。	2005 年 12 月 20 日
	13	「BBSNote」におけるクロスサイト・スクリプティングの脆弱性	ウェブ掲示板「BBSNote」には、投稿データ表示に関するエスケープ処理に漏れがあります。そのため、投稿内容に任意のスクリプトが埋め込まれる可能性があります。	2005 年 12 月 27 日
その他	14	携帯電話の Web ブラウザにおける Referer ヘッダの扱いに関する問題	携帯電話によるインターネット接続サービスのブラウザに、送信すべきでない状況において、Referer 情報を送信してしまう問題が確認されました。	2005 年 12 月 9 日

⑵ 海外 CSIRT から連絡を受け公表した脆弱性

表 2-3 および表 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。2005 年第 4 四半期は、米国 CERT/CC から 10 件、英国 NISCC (National Infrastructure Security Co-ordination Centre) から 1 件の合計 11 件の脆弱性関連情報の連絡を受けました。このほかに、6 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	Snort Back Orifice プリプロセッサにバッファオーバーフローの脆弱性	単独製品開発者に展開
2	Clam AntiVirus におけるバッファオーバーフローの脆弱性	JVN 掲載
3	unace にバッファオーバフローの脆弱性	JVN 掲載
4	Cisco IOS に heap integrity checks を迂回される脆弱性	単独製品開発者に展開
5	Skype の URI ハンドラにバッファオーバーフローの脆弱性	JVN 掲載
6	Skype にヒープオーバーフローの脆弱性	JVN 掲載
7	Skype VCARD handling routine にバッファオーバーフローの脆弱性	JVN 掲載
8	TCP プロトコルに Optimistic TCP acknowledgements による DoS が可能な脆弱性	複数製品開発者に展開
9	Microsoft Internet Explorer の"Window()"オブジェクトの処理に任意のコード実行の脆弱性	JVN 掲載
10	Symantec 製品に含まれる RAR アーカイブ解凍ライブラリにヒープオーバーフローの脆弱性	単独製品開発者に展開

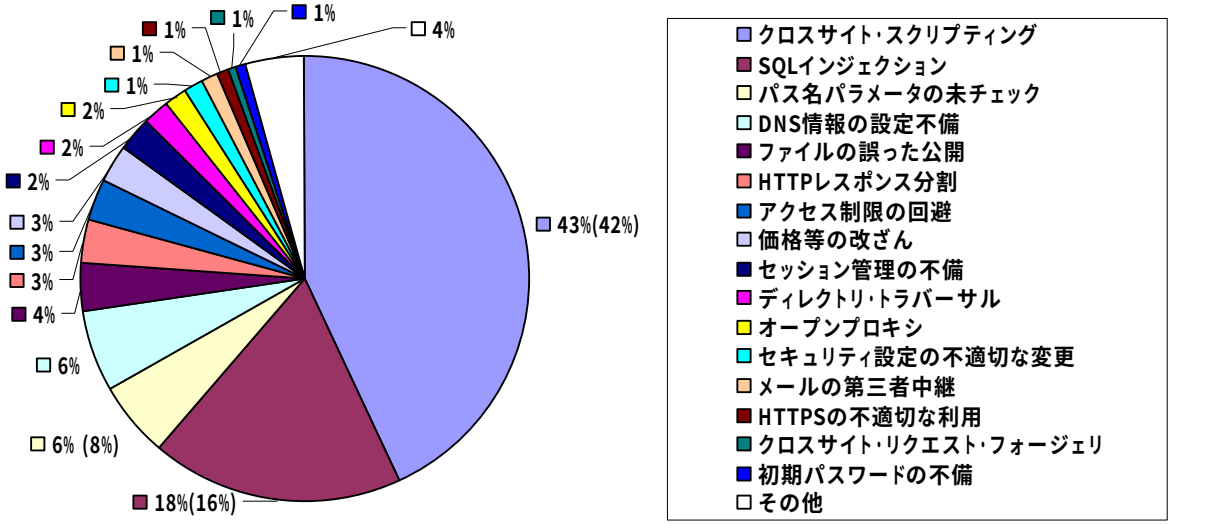
表 2-4 NISCC から連絡を受けた脆弱性関連情報

項番	脆 弱 性	対応状況
1	ISAKMP プロトコルの実装に複数の脆弱性	複数製品開発者に展開

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435件のうち、不受理のものを除いた409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。

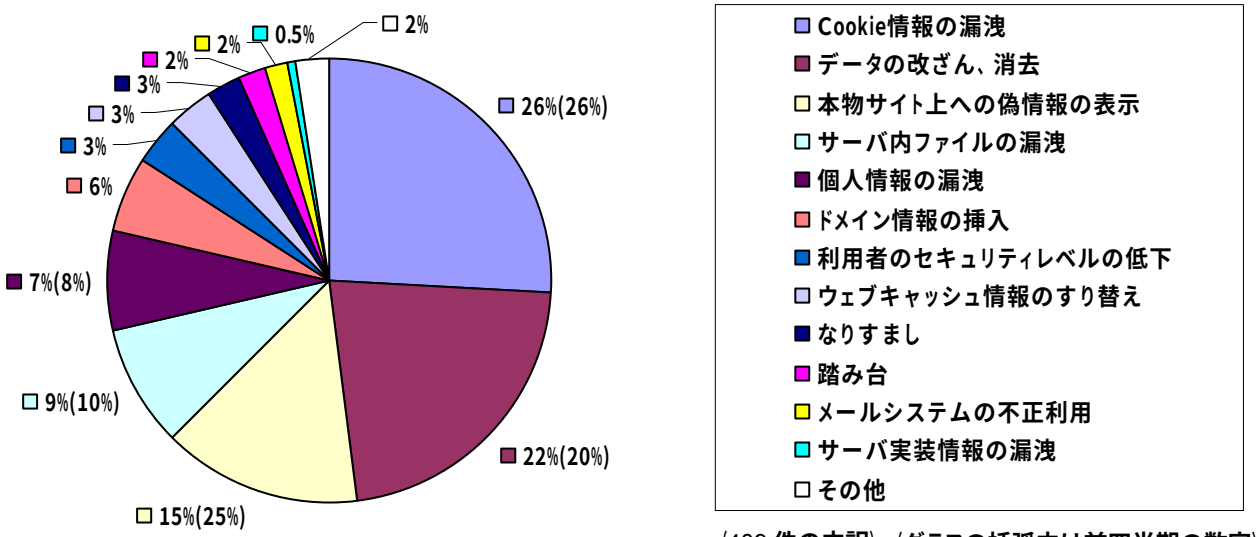


(409件の内訳)　(グラフの括弧内は前四半期の数字)

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2005年12月末まで)[5]

図3-1から、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」が最多でしたが、「SQLインジェクション」が増加しています。

「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46件のうち、27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19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。



(409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2005年12月末まで)

[5] 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。

図 3-2 から、発見者が届出時に想定した脅威別では、「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」が最多であり、「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」、「DNS 情報の設定不備」により起こりうる「ドメイン情報の挿入」が増加しています。

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 2005 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 85%の届出が、100 日以内に修正されています。

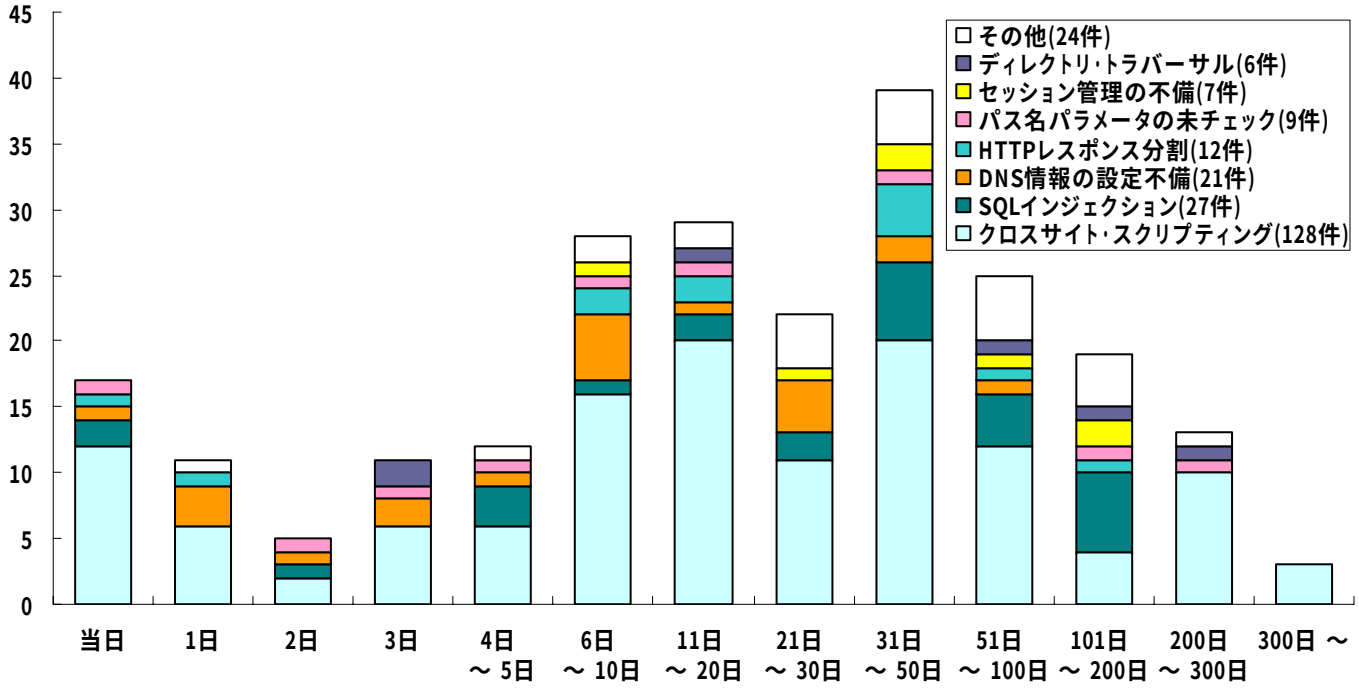


図 3-3 ウェブアプリケーションの脆弱性修正に要した日数

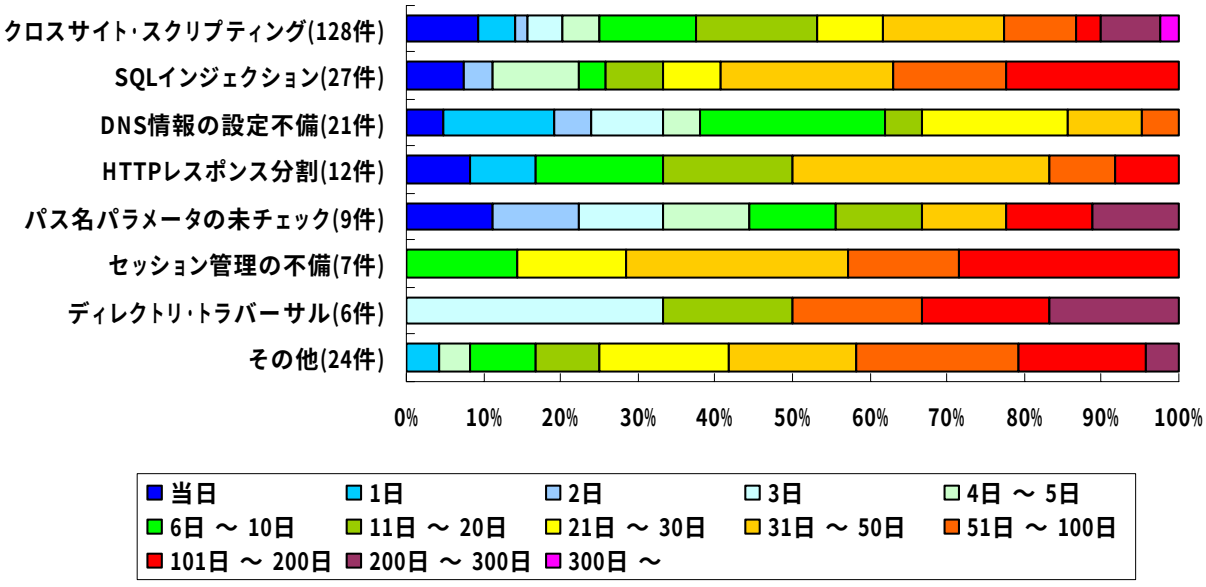


図 3-4 ウェブアプリケーションの脆弱性別 修正に要した日数

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およびシステム構築事業者の皆様へ

  「SQL インジェクション」の届出があったウェブサイトのうち、約 6 割のウェブサイトで、SQL エラー表示がでているだけでなく実際に SQL コマンドが挿入できる状態にあったという結果になっています。あらためて、お使いのウェブアプリケーションを確認されることを、推奨します。

- 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。

■ 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 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	価格等の改ざん サービス不能 資源の枯渇 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 任意のコードの実行 任意のコマンドの実行 任意のスクリプトの実行 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	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	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
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 任意のスクリプトの実行 任意のファイルへのアクセス

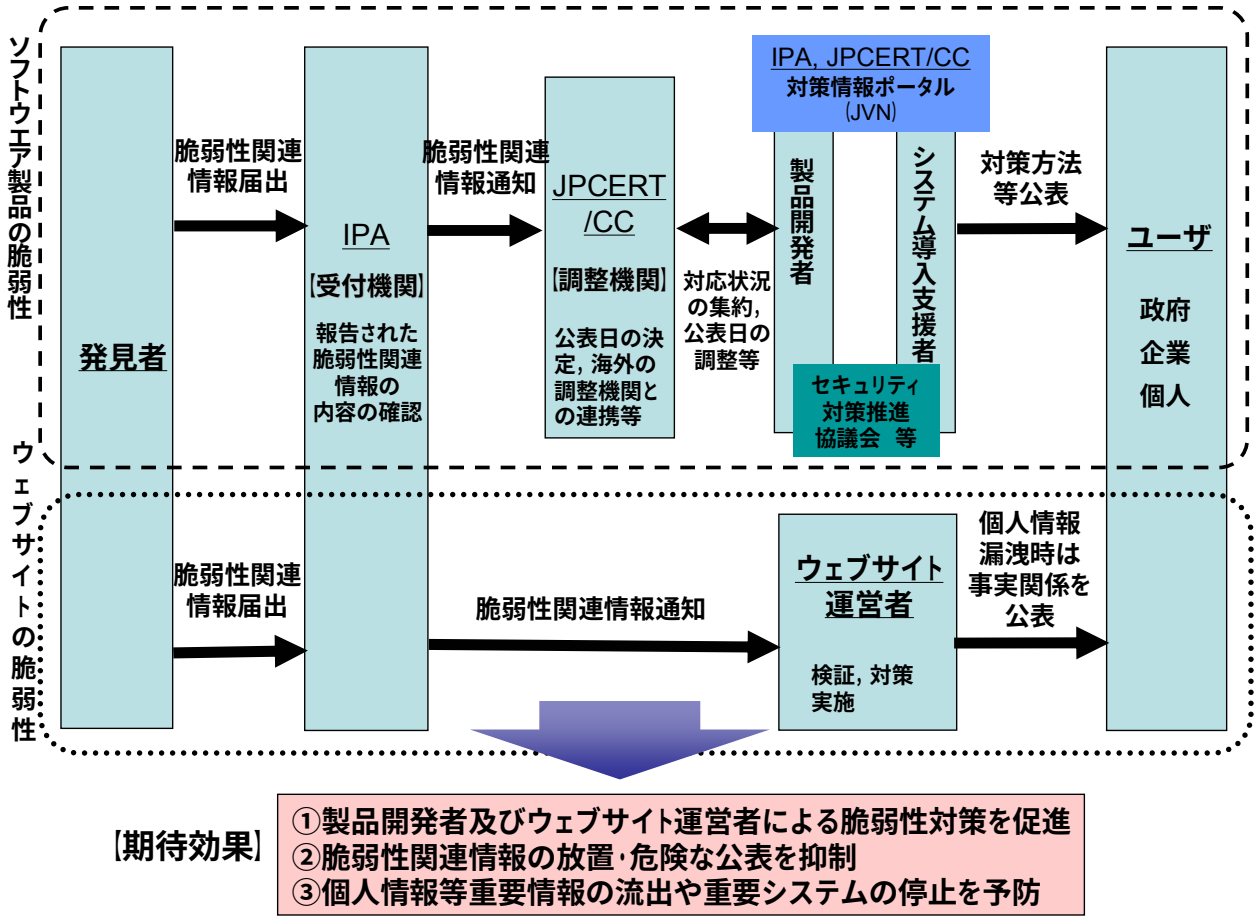
付表 2 ウェブアプリケーション脆弱性の分類

	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	サーバ内ファイルの漏洩 個人情報の漏洩
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	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	個人情報の漏洩 権限の無い者によるサービス利用
5	SQL コマンド・インジェクション	高	入力フォームへ 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	サーバ内ファイルの漏洩 データの改ざん、消去
6	SSI インジェクション	高	入力フォームなどへ悪意のある SSI コマンドを入力し、ウェブサーバ上での OS コマンドの実行や、非公開のファイルの表示ができる	サーバ内ファイルの漏洩
7	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
8	アクセス制限の回避	中	本来設けられているアクセス制御機能による制限を回避し、制限により行えないはずの活動ができてしまう	利用者のセキュリティレベルの低下
9	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
10	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 本物サイト上への偽情報の表示
11	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
13	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

	脆弱性の種類	深刻度	説明	届出において想定された脅威
14	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
15	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	第三者への DoS 攻撃
16	初期パスワードの不備	低	認証に使用するために、管理者が発行したユーザ ID や初期パスワードが、単純であり推測が容易である、または、パスワードそのものを使用していない	個人情報の漏洩
17	不適切なエラー処理	低	表示されるエラーの内容に、一般ユーザには不要な情報が含まれているため、ウェブサイトの実装の詳細や、ファイルやユーザの有無がわかる	サーバ実装情報の開示
18	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	データの改ざん
19	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

API : Application Program Interface
CGI : Common Gateway Interface
HTTP : HyperText Transfer Protocol
HTTPS : Hypertext Transfer Protocol Security
ISAKMP : Internet Security Association Key Management Protocol
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脆弱性関連情報の放置・危険な公表を抑制
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

出典：脆弱性関連情報取り扱い説明会資料　「ソフトウエア等脆弱性関連情報取扱基準とガイドラインの概要説明」，経済産業省（2004年7月）