IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

プレスリリース
2005 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 [2005 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「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 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。

- ソフトウエア製品の脆弱性関連情報
  届出　　：18 件 (届出受付開始からの累計は 62 件)
  脆弱性公表：12 件 (届出受付開始からの累計は 29 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　　：66 件 (届出受付開始からの累計は 277 件)
  修正完了　：33 件 (届出受付開始からの累計は 124 件)

1. 届出件数[1]

2005 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、84 件 (ソフトウエア製品に関するもの 18 件、ウェブアプリケーションに関するもの 66 件) であり、届出受付開始 (2004 年 7 月 8 日) からの累計は 339 件 (ソフトウエア製品に関するもの 62 件、ウェブアプリケーションに関するもの 277 件) です。四半期毎の届出状況を表 1-1 に示します。

表 1-1 脆弱性関連情報の四半期別届出件数の推移

	2004/3Q (7～9 月)	2004/4Q (10～12 月)	2005/1Q (1～3 月)	2005/2Q (4～6 月)	合計
ソフトウエア製品に関する届出	19	13	12	18	62
ウェブアプリケーションに関する届出	73	67	71	66	277
合 計	92	80	83	84	339

(注：就業日 1 日あたり 1.42 件)

[1] 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。

(1) ソフトウエア製品の脆弱性

IPAに届出られたソフトウエア製品の脆弱性関連情報について、届出の取扱い状況を図 1-1 に示します。図 1-1 に示すとおり、2005 年第 2 四半期中に公表[2]した脆弱性は、**12 件** (累計 **29 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 8 件 (累計 11 件) 、不受理としたものは 2 件 (累計 6 件) ありました。

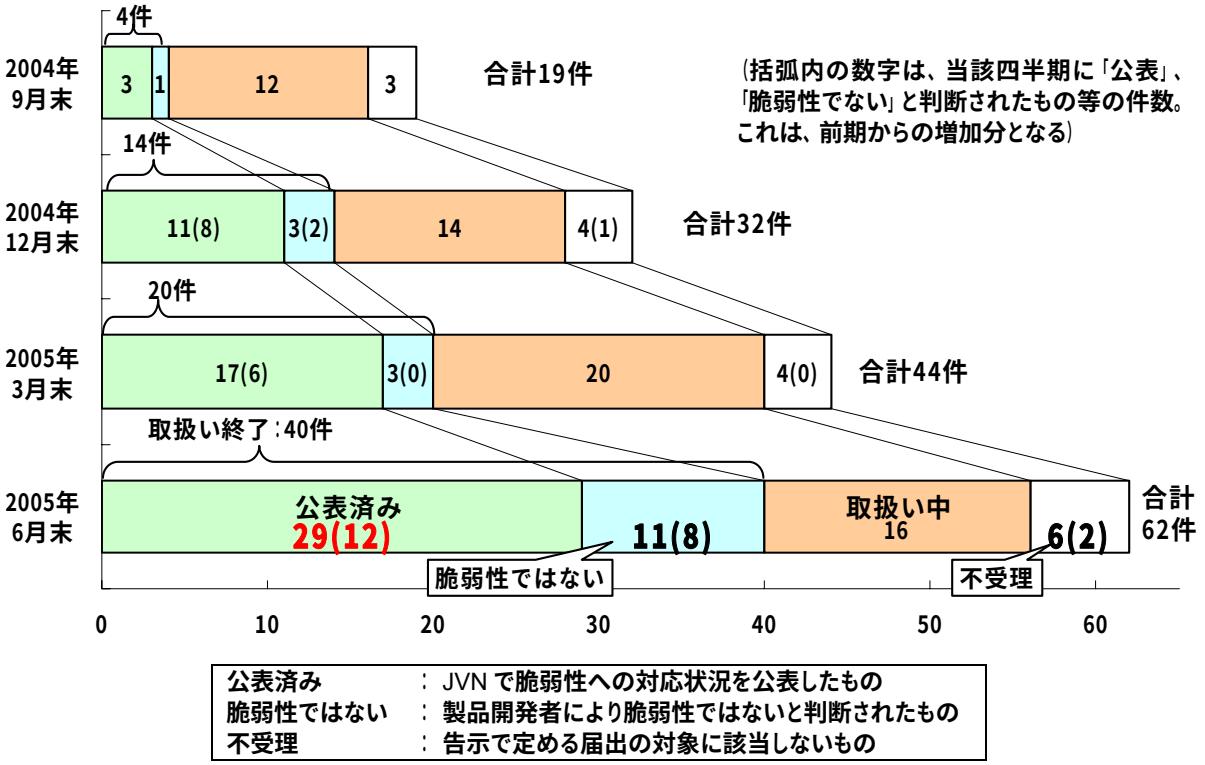


図 1-1 ソフトウエア製品 各時点における脆弱性関連情報の届出の取扱い状況

この他に、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。

(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の脆弱性関連情報の届出について、取扱い状況を図 1-2 に示します。

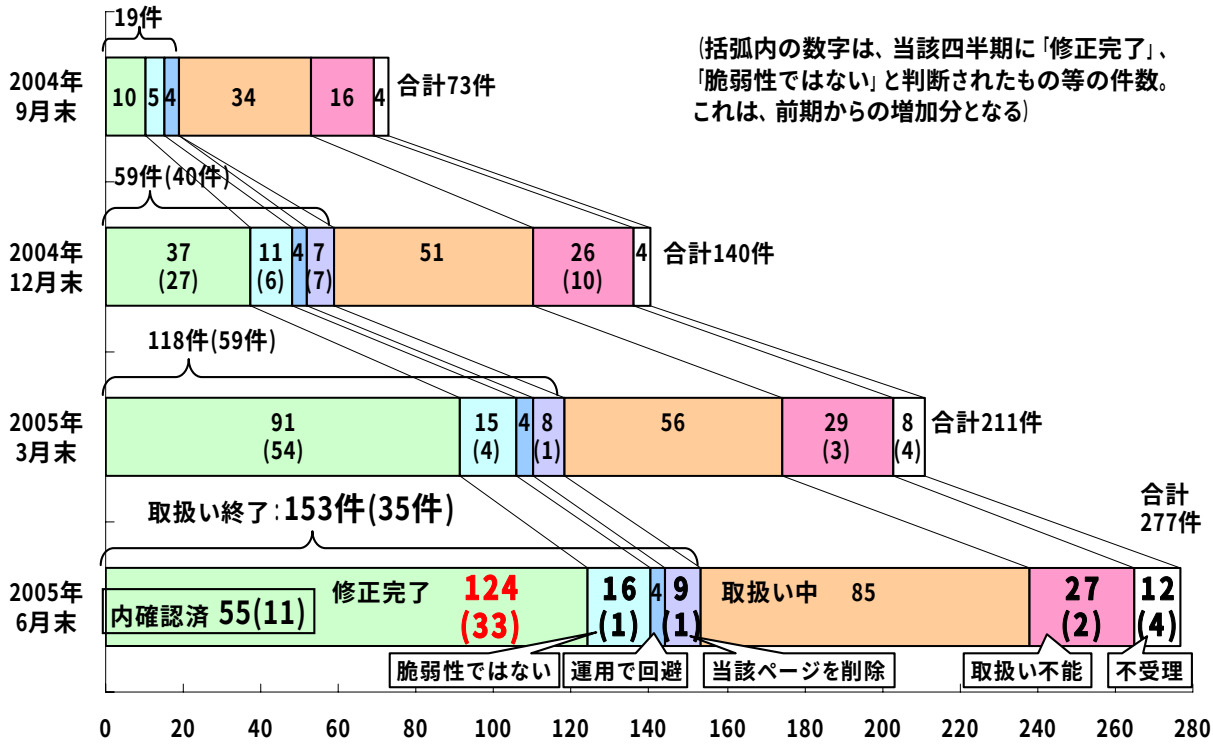
図 1-2 に示すとおり、ウェブアプリケーションの脆弱性については、2005 年第 2 四半期中に取扱いを終了したものは 35 件 (累計 153 件) でした。このうち、修正が完了したものは **33 件** (累計 **124 件**) であり、そのうちの 11 件はウェブサイト運営者からの依頼により IPA が修正確認作業を実施しました (累計 55 件) 。ウェブサイト運営者により脆弱性はないと判断されたものは 1 件 (累計 16 件) 、修正ではなく当該ページを削除することで対応されたものが 1 件 (累計 9 件) ありました。

このほか、取扱い不能 (ウェブサイト運営者と連絡が取れず、取扱いができない状態) になったものが 2 件 (累計 27 件[3]) 、不受理としたものが 4 件 (累計 12 件) ありました。

---

[2] 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。

[3] これまでに取扱い不能となった件について再度連絡を試み、今期末時点で、1 件が修正完了し、3 件はウェブサイト運営者による確認中です。

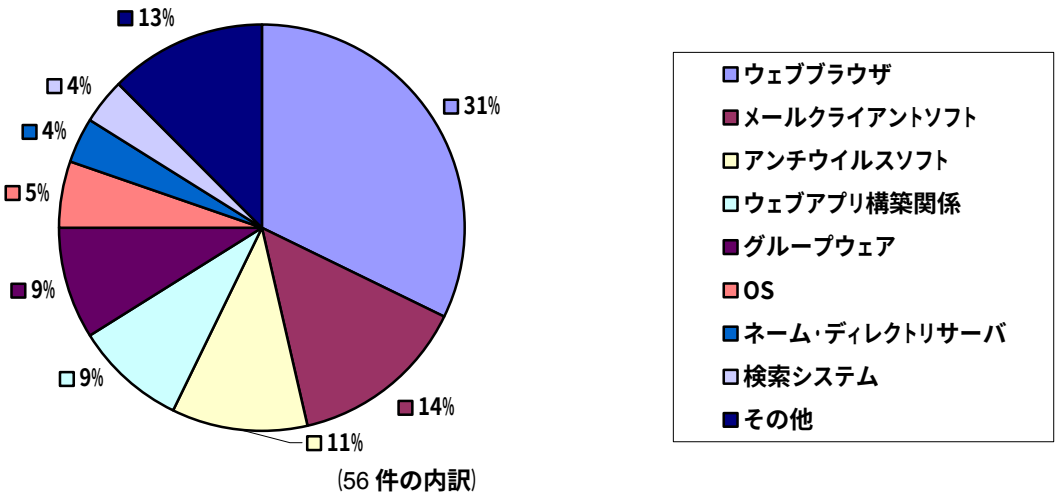


修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
脆弱性ではない	：	ウェブサイト運営者により脆弱性はないと判断されたもの
運用で回避	：	修正はせず、運用により被害を回避しているもの
当該ページを削除	：	修正ではなく当該ページを削除することで対応されたもの
取扱い不能	：	ウェブサイト運営者と連絡が取れず、取扱いができないもの
不受理	：	告示で定める届出の対象に該当しないもの

図 1-2 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取扱い状況

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

届出受付開始から今四半期までに IPA に届出のあったソフトウエア製品に関する脆弱性関連情報の届出 62 件のうち、不受理のものを除いた 56 件の製品種類別の内訳を図 2-1 に示します。



(56 件の内訳)

※1 件のものはその他に分類しています。
ウェブサーバ、SSL-VPN ソフト、プロキシサーバ、システム管理ソフト、情報家電、携帯機器、ルータがあります

図 2-1 ソフトウエア製品種類別の届出件数の内訳 (届出受付開始から 2005 年 6 月末まで)

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/)。

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)	12	29
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	2
③	海外 CSIRT から連絡を受けたもの	17	57
	計	29	88

(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

表 2-2 に脆弱性関連情報の届出 (表 2-1 の①) の受理から、脆弱性およびその対応状況を JVN に公表するまでの平均日数 (平均公表日数) を示します。今四半期に公表した脆弱性の平均公表日数は 115 日、届出受付開始からの全ての公表済み脆弱性の平均公表日数は 88 日となりました。今期公表した脆弱性 12 件のうち、4 件が 1 ヶ月以内に対策され公表された一方、2 件が海外拠点の開発のため調整や修正に 9 ヶ月以上を要しており、公表までの日数の両極化が見られます。

表 2-2 ソフトウエア製品の脆弱性 平均公表日数

	2004/3Q	2004/4Q	2005/1Q	2005/2Q
当該期公表分	49	43	101 [5,6]	115 [6]
通算	49	45	71 [5,6]	88 [6]

表 2-3 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 2 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。今四半期に公表した脆弱性の多くは、ウェブに関連したソフトウエア製品に関するものでした。そのため、クロスサイト・スクリプティングなど、ウェブアプリケーションと同様の問題が多くありました。

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、≪「nProtect ： Netizen」に複数の脆弱性≫ (表 2-3 項番 1) 、≪「Wiki」クローン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) 、≪メールクライアントソフトにおける mailto URL scheme の不適切な解釈≫ (項番 3) の 3 件であり、特定の製品に関する脆弱性は 9 件でした。≪「WebUD」における任意のプログラムが実行される脆弱性≫ (項番 4) 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、≪携帯電話端末における特定 QR (Quick Response) コードを使用したサイト接続時の問題≫ (項番 13) 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。

---

[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。

[5] 前期の日数に誤りがありましたので、訂正しました。

[6] 海外で開発されている製品のため、調整、修正に長期間を要したものを含みます。

表 2-3 2005 年第 2 四半期に公表した脆弱性

	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	「nProtect : Netizen」に複数の脆弱性	ウイルス・不正アクセス・フィッシング詐欺対策のためのセキュリティツール「nProtect : Netizen」において、脆弱性が確認されました。利用者が、悪意あるウェブページを閲覧してしまった際に、悪意あるファイルの保存、ブラウザの強制終了などの被害を受ける可能性があります。	2005 年 4 月 25 日
	2	「Wiki」クローン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うウェブコンテンツ管理システム「Wiki」のいくつかの実装において、「ファイル添付機能」にクロスサイト・スクリプティングの脆弱性が確認されました。利用者のブラウザ上でスクリプトが実行され、Cookie が盗まれる可能性があります。	2005 年 5 月 19 日
	3	メールクライアントソフトにおける mailto URL scheme の不適切な解釈	いくつかのメールクライアントにおいて、解釈すべきでないメールヘッダを解釈する問題が確認されました。これにより、利用者が気づかずに第三者にメールを送信してしまう可能性があります。	2005 年 5 月 26 日
特定製品の脆弱性	4	「ppBlog」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「ppBlog」において、クロスサイト・スクリプティングの脆弱性が確認されました。利用者のブラウザ上でスクリプトが実行され、Cookie が盗まれる可能性があります。	2005 年 4 月 11 日
	5	バッファロー製ルータにおける設定画面のリモートアクセスとパスワード漏洩の脆弱性	バッファロー製ルータの一部に、WAN 側からリモートアクセスできる脆弱性が確認されました。遠隔の第三者に管理画面にアクセスされたり、管理画面の設定保存機能から ISP へ接続するためのユーザアカウントやパスワードを取得される可能性があります。	2005 年 4 月 15 日
	6	「w3ml」におけるクロスサイト・スクリプティングの脆弱性	メーリングリストへの投稿メールを蓄積し、ウェブブラウザで参照できるようにするためのプログラム「w3ml」において、クロスサイト・スクリプティングの脆弱性が確認されました。利用者のブラウザ上でスクリプトが実行され、Cookie が盗まれる可能性があります。	2005 年 4 月 19 日
	7	「WebUD」における任意のプログラムが実行される脆弱性	ウェブ・アクセシビリティ支援ツール「WebUD」において、「WebUD」上で自動実行される部品に脆弱性が確認されました。これにより、利用者が悪意のあるサイトにアクセスしてしまった際に、利用者のコンピュータ上で任意のプログラムが実行される可能性があります。	2005 年 4 月 22 日
	8	「Movable Type」におけるセッション管理の脆弱	ウェブログを作成・管理するためのシステム「Movable Type」において、セッション情報を不適切に取り扱う脆弱性が確認されました。悪意あるユーザが、正規にログインした利用者のセッション情報を盗むことにより、ログイン認証を回避してウェブログへの投稿や削除を行う可能性があります。	2005 年 5 月 12 日
	9	「ウイルスセキュリティ」におけるヒープオーバーフローの脆弱性	「ウイルスセキュリティ」の e メール自動監視機能において、特別に細工されているウイルス添付メールを受信すると、監視処理が異常終了してしまう脆弱性が確認されました。一定期間、メールの受信ができなくなる可能性があります。	2005 年 5 月 12 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
	10	「ウイルスセキュリティ」におけるメモリリークの脆弱性	「ウイルスセキュリティ」の e メール自動監視機能において、特別に細工されているメールを受信すると、この監視処理が異常終了してしまう脆弱性が確認されました。一定期間、メールの受信ができなくなる可能性があります。	2005 年 5 月 13 日
	11	「desknet's」におけるクロスサイト・スクリプティングの脆弱性	ウェブグループウェア「desknet's」のウェブメール機能において、クロスサイト・スクリプティングの脆弱性が確認されました。利用者のブラウザ上でスクリプトが実行され、Cookie (設定によっては ID やパスワードを含む) が盗まれる可能性があります。	2005 年 6 月 6 日
	12	「SFS」におけるクロスサイト・スクリプティングの脆弱性	ウェブフィルタリングシステム「SFS」において、クロスサイト・スクリプティングの脆弱性が確認されました。利用者のブラウザ上でスクリプトが実行され、Cookie が盗まれる可能性があります。	2005 年 6 月 10 日
その他	13	携帯電話端末における特定 QR コードを使用したサイト接続時の問題[7]	2 次元コード (QR コード) 読みとり機能を搭載している携帯電話端末において、特定の QR コードを読み込んだ際に、2 行表示される文字列 (URL 等) の 1 行目に接続しようとすると、2 行目の URL に接続する問題が確認されています。	2005 年 4 月 14 日

⑵ 海外 CSIRT から連絡を受け公表した脆弱性

表 2-4 および表 2-5 に、海外 CSIRT から連絡を受けた脆弱性を示します。2005 年第 2 四半期は、米国 CERT/CC から 12 件、英国 NISCC (National Infrastructure Security Co-ordination Centre) から 5 件の合計 17 件の脆弱性関連情報の連絡を受けました。

表 2-4 CERT/CC から連絡を受けた脆弱性関連情報

項番	脆 弱 性	調整先
1	Microsoft Windows コンポーネントに存在する複数の脆弱性	なし
2	複数の Telnet クライアントに env_opt_add() を通したバッファオーバーフローの脆弱性	複数製品開発者
3	複数の Telnet クライアントに "LINEMODE" SLC suboption の処理に関する脆弱性	複数製品開発者
4	sendfile() システムコールにおけるカーネルメモリ漏洩の脆弱性	複数製品開発者
5	Bluetooth をサポートする Linux カーネルにおける "protocol" 値の処理に関する脆弱性	複数製品開発者
6	オラクル製品に複数の脆弱性	なし
7	Apple の Mac OS X に複数の脆弱性	なし
8	TCP の実装に不正な値で内部タイマを更新する脆弱性	複数製品開発者
9	simultaneous multithreading プロセッサにおける機密情報漏洩の可能性	複数製品開発者
10	Microsoft Windows および Internet Explorer に存在する複数の脆弱性	なし
11	VERITAS Backup Exec Remote Agent の認証要求の確認機能に脆弱性	複数製品開発者
12	VERITAS Backup Exec Remote Agent の脆弱性を対象とする侵害活動	なし

[7]製品開発者の判断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へ掲載しているため、「公表済み」として分類しています。

表 2-5 NISCC から連絡を受けた脆弱性関連情報

項番	脆 弱 性	調整先
1	Adobe Reader control の脆弱性	なし
2	TCP 実装の ICMP エラーメッセージの処理に関する脆弱性	複数製品開発者
3	IPSec 通信の設定に存在する脆弱性	複数製品開発者
4	DNS パケットに含まれる圧縮されたデータの展開処理に関する脆弱性	複数製品開発者
5	複数のウェブブラウザに存在する画像データの処理に関する脆弱性	複数製品開発者

3. ウェブアプリケーションの脆弱性関連情報の取扱い

届出受付開始から今四半期末までに IPA に届出のあったウェブアプリケーションに関する脆弱性関連情報の届出 277 件のうち、不受理のものを除いた 265 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。

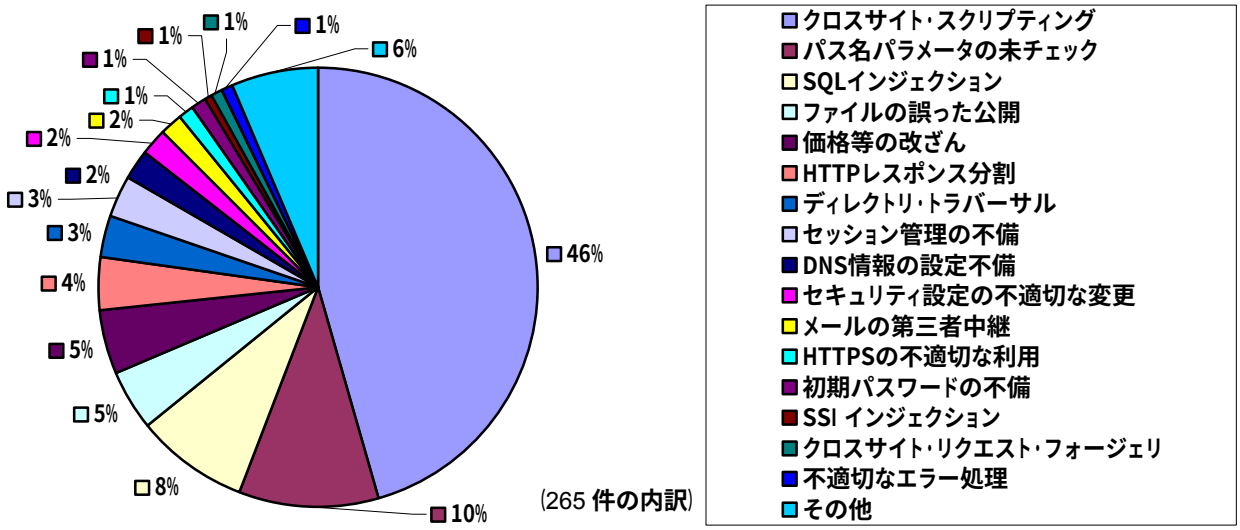


図 3-1 ウェブアプリケーションの脆弱性種類別内訳 (届出受付開始から 2005 年 6 月末まで)

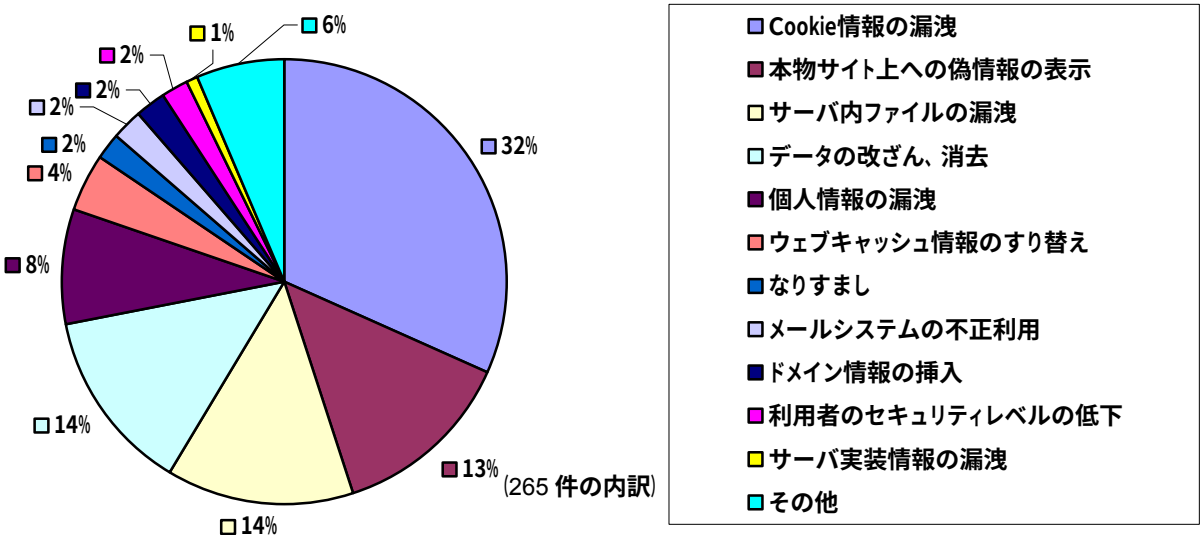


図 3-2 ウェブアプリケーションの脆弱性脅威別内訳 (届出受付開始から 2005 年 6 月末まで)

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」が最多であり、図 3-2 から、発見者が届出時に想定した脅威別では、この脆弱性により起こりうる「Cookie 情報の漏洩」が最多であることがわかります。

2005 年第 2 四半期の届出として、「DNS[8]情報の設定不備」の問題がありました。これは、DNSサーバの設定に不備があるため、第三者にドメイン情報を挿入される可能性があり、それによりフィッシング詐欺や情報漏洩につながる可能性があるというものでした。

また、今期は、ウェブサイトの改ざんによるウイルス被害など、ウェブサイトの脆弱性の悪用による情報漏えいやウェブページ改ざんなどが頻発しました。

このため、IPA では、ウェブサイト運営者がウェブサイトや自ドメインの DNS サーバについて、セキュリティ対策や設定、登録内容の確認ができるよう、注意喚起資料を公表しました。

「ドメイン名の登録と DNS サーバの設定に関する注意喚起」
http://www.ipa.go.jp/security/vuln/20050627_dns.html

「ウェブサイトのセキュリティ対策の再確認を ～脆弱性対策のチェックポイント～」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

届出受付開始から 2005 年 6 月末までの届出について、修正された脆弱性の種類別件数および修正に要した日数を図 3-3 に示します。

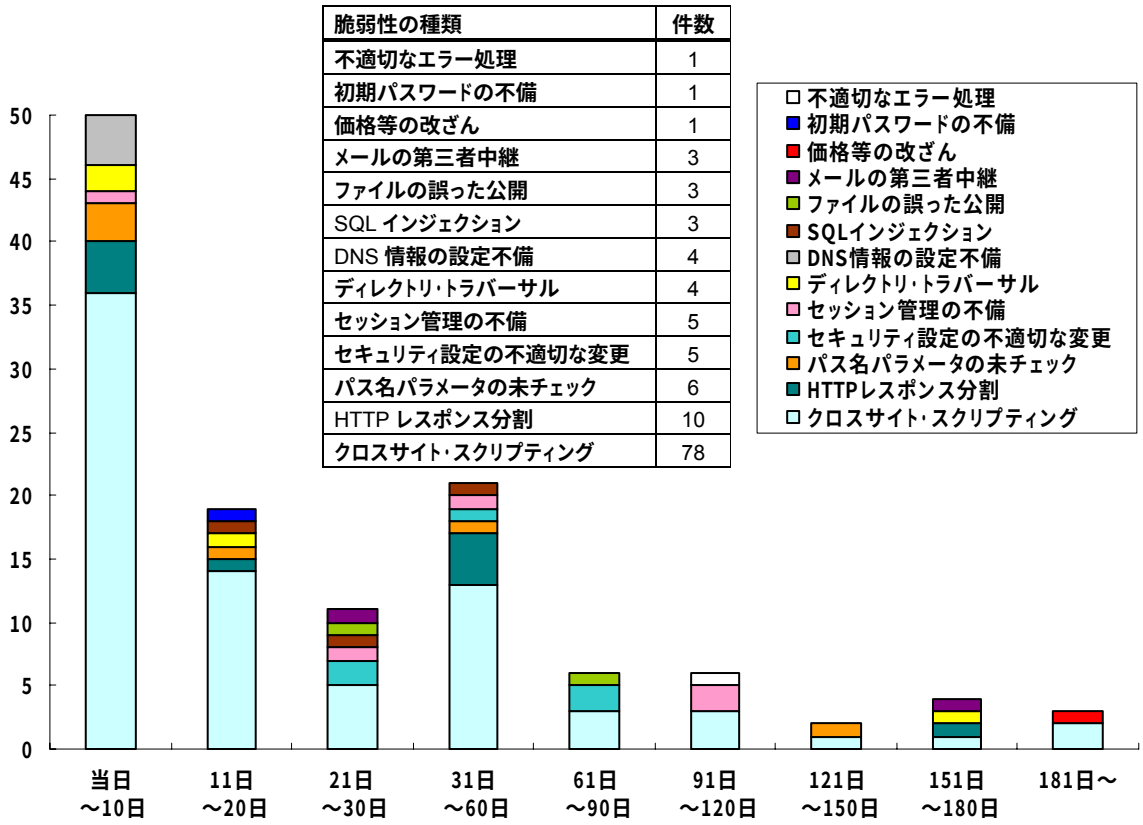


図 3-3 ウェブアプリケーションの脆弱性修正に要した日数

[8] DNS (Domain Name System) は、インターネット上の住所であるIPアドレスとホスト名 (例：www.ipa.go.jp) を変換するための仕組みです。

4. 皆様へのお願い

脆弱性の修正を促進していくため、関係者の皆様に、以下のとおり、ご協力をお願いします。

- 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

  ウェブサイトの脆弱性の悪用による被害を回避するためには、ウェブアプリケーション、ウェブアプリケーションが稼動しているウェブサーバ、ウェブサーバが設置されているネットワーク（ルータやファイアウォール）のセキュリティ対策が必要です。さらに、データベースを利用している場合は、ウェブアプリケーションの脆弱性によりデータベースへアクセスされないように対策しておく必要があります。総合的なセキュリティ対策を採ることを、推奨します。

- 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、対策情報の公表の際には、利用者が脆弱性を認識し、必要な対策が取れるよう、適切な情報を伝えるようにしてください。

- 脆弱性を発見された皆様へ

  脆弱性を発見した場合は、匿名掲示板などに書き込むことは避け、この届出制度を利用してください。また、届け出た情報は、その脆弱性に関する情報が悪意のある者に利用されることを避けるため、開発者等により対策情報が公表されるまで、公表しないよう、お願いします。

- 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。使用しているブラウザによっては、ウェブサイトを対象によってグループ分けし、セキュリティレベルを設定することができます。セキュリティレベルを低く設定していると、悪意あるウェブサイトを閲覧しただけでプログラムがインストールされてしまうこともありますので、安易に低い設定にしないよう、注意してください。

■ 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

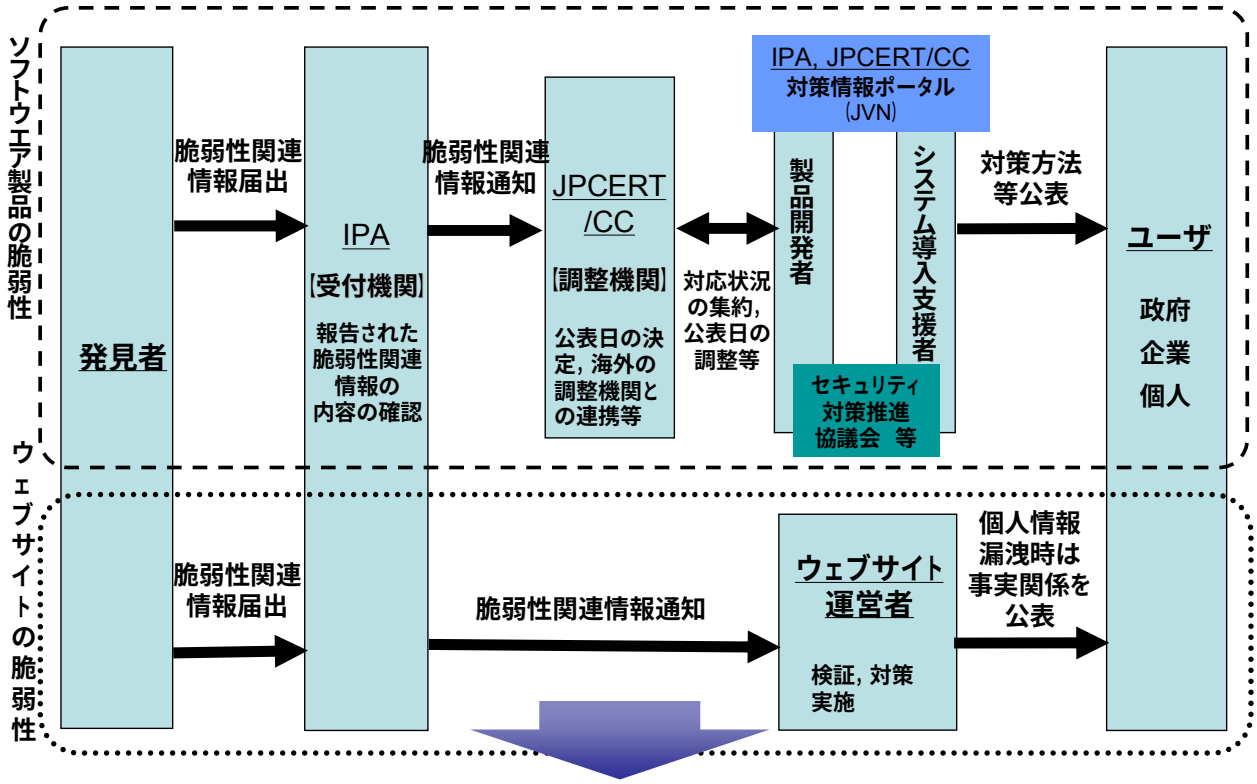
付表 1 ウェブアプリケーション脆弱性の分類

脆弱性の種類	深刻度	説明	届出において想定された脅威
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
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
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
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
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
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
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
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
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
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
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
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

脆弱性の種類	深刻度	説明	届出において想定された脅威
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
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
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
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

HTTP :HyperText Transfer Protocol
HTTPS :Hypertext Transfer Protocol Security
ICMP :Internet Control Message Protocol
IPSec :Internet Protocol security
ISP :Internet Service Provider
SLC :Set Local Character
SQL :Structured Query Language
SSI :Server Side Include
SSL :Secure Socket Layer
TCP :Transmission Control Protocol
URL :Uniform Resource Locator
VPN :Virtual Private Network
WAN :Wide Area Network

「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：報道資料”「情報セキュリティ総合戦略」策定について”，経済産業省（2003年10月10日）