IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

プレスリリース
2005 年 4 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 1 四半期 (1 月～3 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、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。今般、2005 年第 1 四半期 (1 月～3 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。

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 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開始しました。2005 年第 1 四半期 (1 月～3 月) の脆弱性関連情報の届出状況は以下のとおりです。

- ソフトウエア製品の脆弱性関連情報
  届出　　：12 件 (届出受付開始からの累計は 44 件)
  脆弱性公表： 6 件 (届出受付開始からの累計は 17 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　　：71 件 (届出受付開始からの累計は 211 件)
  修正完了　：54 件 (届出受付開始からの累計は 91 件)

1. 届出件数[1]

2005 年 1 月 1 日から 3 月 31 日までの IPA への脆弱性関連情報の届出件数は、83 件 (ソフトウエア製品に関するもの 12 件、ウェブアプリケーションに関するもの 71 件) であり、届出受付開始 (2004 年 7 月 8 日) からの累計は 255 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)	合計
ソフトウエア製品に関する届出	19	13	12	44
ウェブアプリケーションに関する届出	73	67	71	211
合 計	92	80	83	255

(注：就業日 1 日あたり 1.45 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 および表 1-2 に示します。

表 1-2 に示すとおり、2005 年第 1 四半期中に公表[2]した脆弱性は、6 件 (累計 17 件) です。今四半期中に、製品開発者により脆弱性ではないと判断されたもの、不受理としたものはありませんでした。脆弱性関連情報の届出受理から、JVNに脆弱性およびその対応状況を公表するまでの平均日数は、今期公表した脆弱性については 71.5 日、届出受付開始からの全ての公表済み脆弱性については 55 日となりました (図 1-1 参照)。

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。

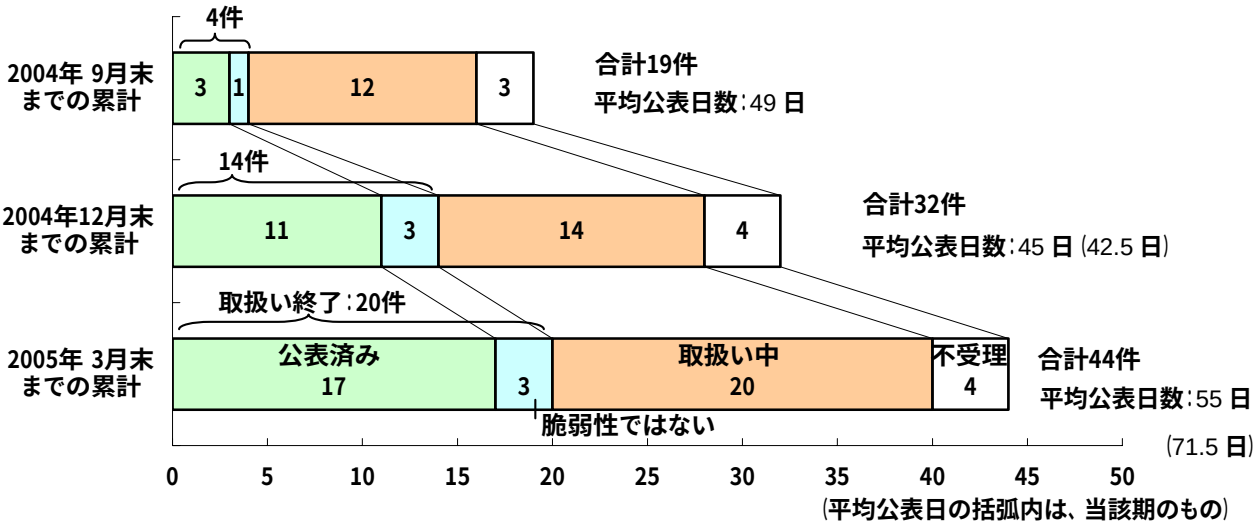


図 1-1 ソフトウエア製品 脆弱性関連情報の届出の取扱い状況

表 1-2 ソフトウエア製品 脆弱性関連情報の届出の取扱い状況

	公表	脆弱性ではない	不受理	取扱い中 (四半期末時点)
2004/3Q	3	1	3	12
2004/4Q	8	2	1	14
2005/1Q	6	0	0	20
合計	17	3	4	

[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。

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、取扱い終了の内訳を表 1-3 に、取扱い状況を図 1-2 および表 1-4 に示します。

表 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、2005 年第 1 四半期中に取扱いを終了したものは 59 件（累計 118 件）でした。このうち、修正が完了したものは 54 件（累計 91 件）であり、そのうちの 23 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 44 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 15 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 8 件）ありました。

このほか、表 1-4 に示すとおり、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 3 件（累計 29 件）、不受理としたものが 4 件（累計 8 件）ありました。

表 1-3 ウェブアプリケーションの脆弱性関連情報 四半期毎の取扱いを終了した届出の内訳

	修正完了	脆弱性ではない	運用で回避	ページを削除	合計
2004/3Q	10	5	4	0	19
2004/4Q	27 (37)	6 (11)	0 (4)	7 (7)	40 (59)
2005/1Q	54 (91)	4 (15)	0 (4)	1 (8)	59 (118)

（括弧内は累計）

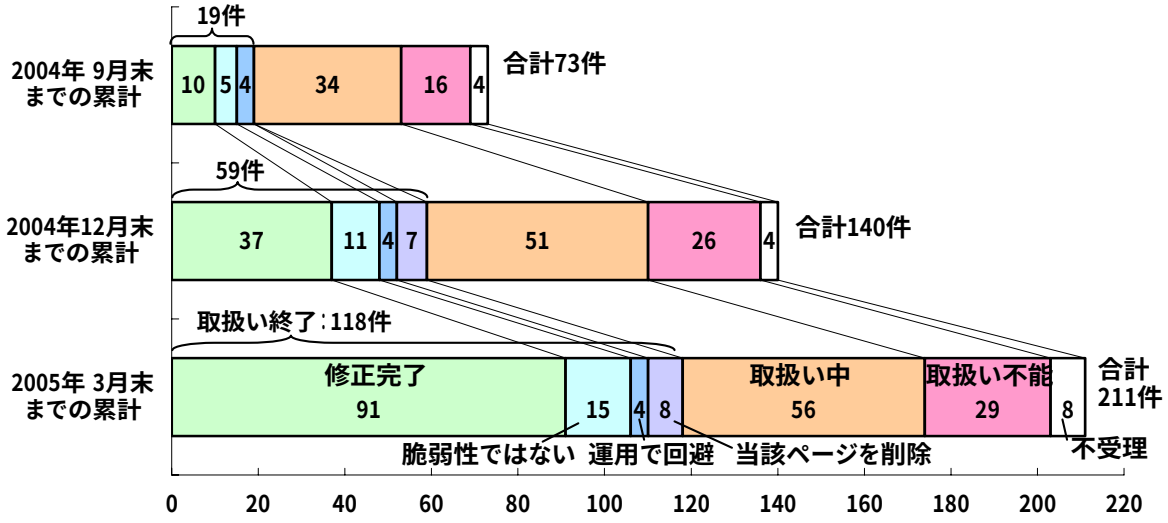


図 1-2 ウェブアプリケーション 脆弱性関連情報の届出の取扱い状況

表 1-4 ウェブアプリケーションの脆弱性関連情報 四半期毎の取扱い状況推移

	取扱い終了	取扱い中（四半期末時点）	取扱い不能	不受理	合計
2004/3Q	19	34	16	4	73
2004/4Q	40	51	10	0	67
2005/1Q	59	56	3	4	71
合計	118		29	8	211

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

JPCERT/CC は、次の 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[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。

① 国内の発見者から IPA に届出があったもの（1（1）に記載）

② 海外 CSIRT から連絡を受けたもの

③ 製品開発者自身から自社製品の脆弱性および対策方法について連絡を受けたもの

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/ ）。今期中に公表した脆弱性は、27 件（累計 57 件）です。このうち、上記①によるものが 6 件（累計 17 件）、②によるものが 20 件（累計 40 件）、③によるものが 1 件（累計 1 件）でした。

ソフトウエア製品に関する脆弱性関連情報の IPA への届出（上記①）の 44 件のうち、不受理のものを除いた 40 件の製品種類別の内訳を、図 2-1 に示します。

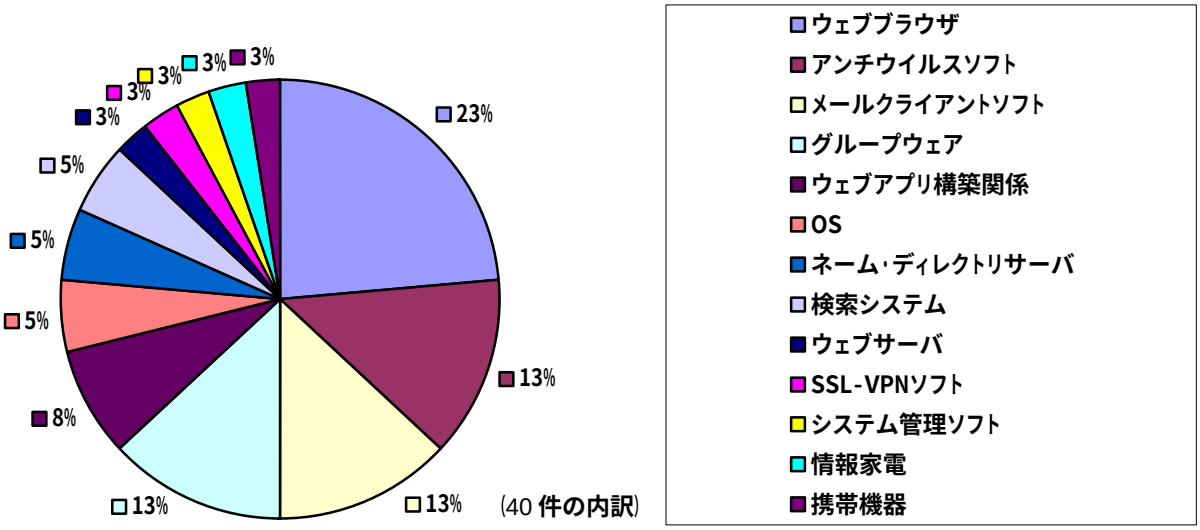


図 2-1 ソフトウエア製品種類別の届出件数の内訳（届出受付開始から 2005 年 3 月末まで）

表 2-1 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 1 四半期に公表した脆弱性（前述の①および③）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ものは、「LDAP[4]サーバの更新機能におけるバッファオーバーフローの脆弱性」（表 2-1 項番 1）、「Tomcatにおけるサービス拒否の脆弱性」（表 2-1 項番 4）の 2 件でした。これらは、一般に広く利用されている技術・製品に関わるもので、海外製品開発者にも影響があるため、JPCERT/CCが海外CSIRT とのパートナーシップに基づき、海外製品開発者も含めて調整し、修正・回避方法の作成が行われました。特定の製品に関する届出の 4 件のうち、アンチウイルスソフト製品に関するものが 2 件、検索システムに関するものが 1 件、グループウェアに関するものが 1 件ありました。「McAfeeウイルススキャンエンジンにバッファオーバーフローの脆弱性」（項番 5）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③）。

---

[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。

[4] LDAP（Lightweight Directory Access Protocol）は、ディレクトリサービスを利用するためのプロトコルであり、多くの人やコンピュータが頻繁に参照する情報を階層型に管理するために利用されます。

表 2-1 2005 年第 1 四半期に公表された脆弱性

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
1	LDAP サーバの更新機能におけるバッファオーバーフローの脆弱性	一部のLDAPサーバの更新処理において、バッファオーバーフローの脆弱性が確認されました。 これにより、遠隔の第三者に、サービス拒否[5]を引き起こされる、また、LDAP サーバの動作権限で任意のコードが実行される可能性があります。	2005 年 1 月 11 日
2	サイボウズ Office におけるブラウザスクリプト実行の脆弱性	サイボウズOfficeのHTML対応ウェブメール機能において、ブラウザスクリプトが実行される脆弱性が確認されました。利用者が、不正なコードを含むウェブメールを開くことにより、サイボウズOfficeへログインするためにブラウザが保持しているCookie[6]情報が漏洩する可能性があります。	2005 年 2 月 7 日
3	msearch におけるディレクトリ・トラバーサルの脆弱性	ウェブページ内全文検索エンジン msearch において、ディレクトリ・トラバーサルの脆弱性が確認されています。これにより、遠隔の第三者に、サーバ内の msearch 設定ファイル、インデックスファイル、これらのファイルと同様の書式で記述されたファイルが、閲覧される可能性があります。	2005 年 3 月 8 日
4	Tomcat におけるサービス拒否の脆弱性	サーバ上で Java アプリケーションを動作させるためのソフトウエアである Apache Jakarta Tomcat において、遠隔から第三者にサービス拒否を引き起こされる脆弱性が確認されました。これにより、サービスの再起動が必要になる可能性があります。	2005 年 3 月 14 日
5	McAfee ウイルススキャンエンジンにバッファオーバーフローの脆弱性	ウイルススキャンエンジンにおいて、不正な圧縮ファイルをスキャンした際に、バッファオーバーフローの脆弱性が確認されました。	2005 年 3 月 18 日
6	Norton AntiVirus で不正なファイルのスキャン時に OS 異常終了	複数のアンチウイルス製品において、ファイルヘッダが不正に細工されたファイルを操作することにより、OS が異常終了する脆弱性が確認されました。	2005 年 3 月 31 日
7	Norton AntiVirus でネットワーク共有ファイルの編集時に OS 異常終了	複数のアンチウイルス製品において、ネットワーク上の共有フォルダ内にあるファイルを編集する際に、OS が異常終了する脆弱性が確認されました。	2005 年 3 月 31 日

[5] コンピュータの負荷の上昇や処理の停止などにより、本来の機能が妨害される問題です。Denial-of-Service, DoSなどと言われ、処理が停止してしまった状態を「DoS状態」、そのような状態を引き起こす攻撃を「DoS攻撃」などと呼びます。

[6] ウェブサーバが発行し、ウェブブラウザに預ける小さなテキストデータです。いったんCookieを預かったウェブブラウザは、それを発行したウェブサーバのコンテンツにアクセスする際、預かったCookieのデータをコンテンツの要求に必ず含めるようになります。ウェブアプリケーションが、どのユーザからのアクセスかを追跡するためにCookieが使われることがあります。その場合、Cookieにはログインの受付番号（場合によってはパスワードそのもの）が格納されるため、Cookie情報が漏洩するとログイン状態を乗っ取られる（セッションハイジャック攻撃に遭う）、またパスワードが漏洩する危険性があります。

表 2-2 に、海外 CSIRT から連絡を受けた脆弱性を示します。2005 年第一四半期は、20 件の脆弱性関連情報の連絡を受け、全て米国 CERT/CC からのものでした。今四半期に英国 NISCC (National Infrastructure Security Co-ordination Centre) から連絡を受けたものはありませんでした。

表 2-2　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	nfs-utils にバッファオーバーフローの脆弱性	複数製品開発者
2	ISC DHCP の errwarn.c にフォーマットストリングの脆弱性	複数製品開発者
3	Microsoft Windows コンポーネントに存在する複数の脆弱性	なし
4	Squid において HTTP レスポンス分割によるキャッシュ汚染の可能性	複数製品開発者
5	Squid における LDAP 認証ルーチンで不正入力チェックが適切に行われない	複数製品開発者
6	Squid において HTTP ヘッダー情報が適切に処理されない	複数製品開発者
7	Squid において大きすぎる応答ヘッダの処理が適切に行われない	複数製品開発者
8	Squid における非常に長い WCCP メッセージに関するバッファオーバーフローの脆弱性	複数製品開発者
9	VERITAS NetBackup の bpjava-susvc で入力が適切に処理されない	複数製品開発者
10	Linux Kernel SMB ファイルシステム read システムコールにバッファオーバーフローの脆弱性	複数製品開発者
11	Veritas Backup Exec にバッファオーバーフローの脆弱性	複数製品開発者
12	UW-imap でユーザ認証が正しく行われない脆弱性	複数製品開発者
13	Cisco IOS にサービス運用妨害 (DoS) 攻撃を受ける複数の脆弱性	なし
14	Juniper にサービス運用妨害 (DoS) 攻撃を受ける脆弱性	なし
15	BIND 9.3.0 の validator にサービス運用妨害 (DoS) 攻撃を受ける脆弱性	複数製品開発者
16	BIND 8.4.4 および 8.4.5 の q_usedns にバッファオーバーフローの脆弱性	複数製品開発者
17	Adobe Acrobat Reader for UNIX にバッファオーバーフローの脆弱性	複数製品開発者
18	LibTIFF に整数オーバーフローの脆弱性	複数製品開発者
19	Microsoft Windows で HTML Help の ActiveX コントロールにクロスドメインの脆弱性	なし
20	Microsoft Windows でアイコンおよびカーソルの処理に複数の脆弱性	なし

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 211 件のうち、不受理のものを除いた 203 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。

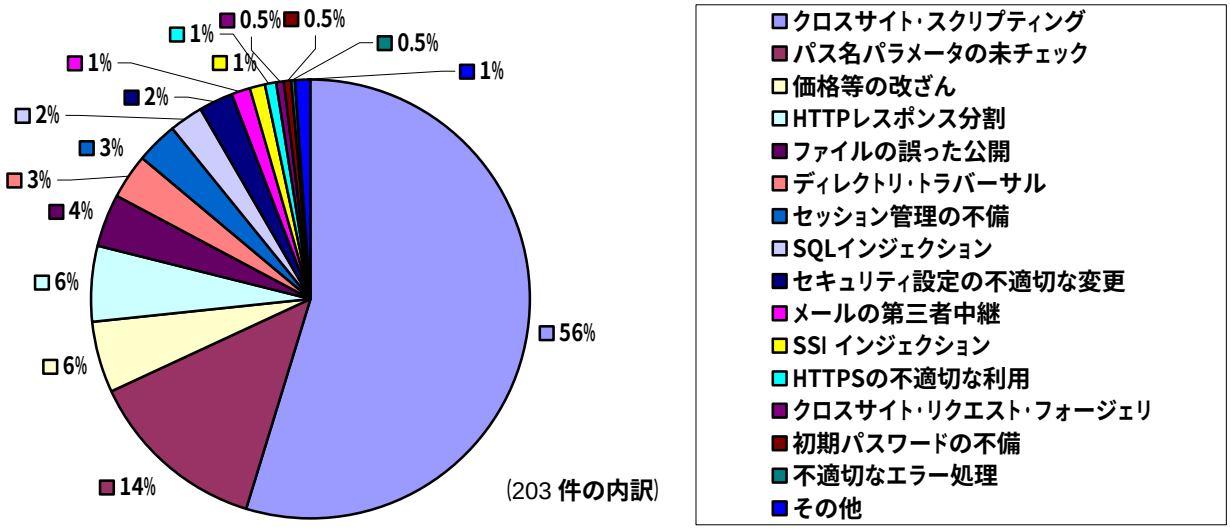


図 3-1 ウェブアプリケーションの脆弱性種類別内訳（届出受付開始から 2005 年 3 月末まで）

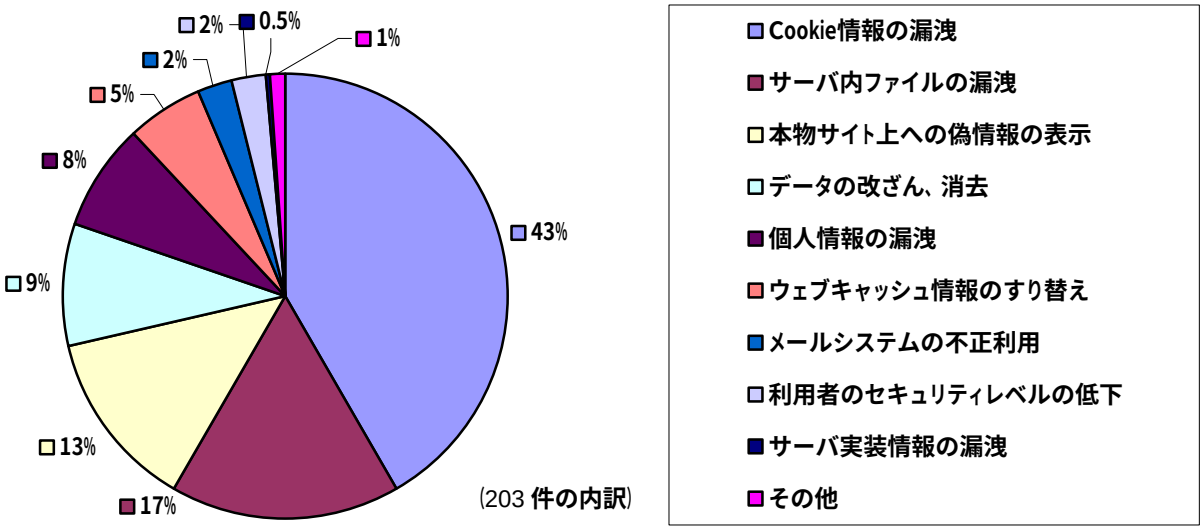


図 3-2 ウェブアプリケーションの脆弱性脅威別内訳（届出受付開始から 2005 年 3 月末まで）

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」が最多となっていることがわかります。また、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。

「クロスサイト・スクリプティング」は、掲示板などの静的なウェブページにスクリプトを埋め込まれる場合に危険であると誤解されることがありますが、検索結果など動的に生成されるページでも、静的なページと同様、スクリプトを埋め込んだページに利用者を誘導することができるため、注意が必要です。

ウェブサイトの脆弱性は、ウェブサイトへの攻撃だけでなく、利用者に対して被害を与えるための罠のページとしても使われます。このような利用者への攻撃に使われた場合、ウェブサイトは意図せず攻撃の一端を担ってしまうことになりますので、注意が必要です。

2005 年第 1 四半期の届出事例として、Java アプリケーション（Java アプレット）のインストールプログラム等がインストール時にクライアント PC の Java 環境のセキュリティポリシーを書換えてしまい、結果として、クライアント PC のセキュリティレベルを低下させてしまう、というものが複数ありました。[7]

また、新たに「SSI[8]インジェクション」「クロスサイト・リクエスト・フォージェリ（Cross-Site Request Forgeries）」の問題を指摘する届出がありました。

「SSI インジェクション」は、入力フォームなどに悪意のある SSI コマンドを入力し、それをウェブアプリケーション宛に送信し実行させることで、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閲覧を試みるものです。「SSI インジェクション」の対策としては、利用者からの入力データをウェブアプリケーションに渡す前に、内容を確認し、問題のある記述を無害化する必要があります。

「クロスサイト・リクエスト・フォージェリ」は、ウェブサイトにアクセスすると自動的にログインするような機能を悪用して、そのウェブサイトの正規の利用者に対し、ユーザ登録内容の変更や意図しない商品購入などをさせるものです。「クロスサイト・リクエスト・フォージェリ」の対策としては、悪用しにくいユーザ登録フォームや商品購入フォームを設計する[9]ことなどが挙げられます。

届出受付開始から 2005 年 3 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表 3-1 に示します。

表 3-1　脆弱性種類別の修正件数および修正に要した日数[10]

脆弱性	件数	修正に要した日数
クロスサイト・スクリプティング（第三者へのスクリプト実行）	64	平均 23 日 (最短：当日、最長：221 日)
パス名パラメータの未チェック（フォーム入力値の操作）	5	平均 13 日 (最短：当日、最長：42 日)
セッション管理の不備	5	平均 60 日 (最短：8 日、最長：119 日)
HTTP レスポンス分割（ウェブサーバ応答内容のすり替え）	4	平均　7 日 (最短：当日、最長：13 日)
SQL インジェクション（データベースへの不正な入力）	3	16 日、27 日、39 日
メールの第三者中継	3	1 日、29 日、159 日
ファイルの誤った公開	2	1 日、21 日
ディレクトリ・トラバーサル（許可されていない範囲へのアクセス）	2	3 日、 3 日
セキュリティ設定の不適切な変更	2	27 日、31 日
不適切なエラー処理	1	97 日

[7] これらは、クライアント PC にインストールするソフトウエアですが、ウェブアプリケーションを使うためのものであり、そのウェブアプリケーションと独立して起動され、使用されるものではないため、ウェブアプリケーションの一部として捉え、ウェブアプリケーションの脆弱性関連情報の届出として取扱いました。

[8] SSI（Server Side Include）は、ユーザがウェブページにアクセスした際に、あらかじめそのページ内に記述されている実行可能コマンドをサーバ側で実行し、その結果をウェブページに反映してユーザに見せる仕組みです。ウェブページ上への時刻の表示やアクセスカウンターの設置などに使うことができます。

[9] この攻撃では HTTP の GET メソッドが使われることが多いため、フォームの処理に POST メソッドのみを使用することで、悪用されにくくなります。

[10] 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。

「クロスサイト・スクリプティング」など、利用者からの入力を無害化していないことに起因する脆弱性についての届出が依然として多いことから、IPA は、一般の利用者がよく利用し、クレジットカード情報等の個人情報を扱うことが多い消費者向け電子商取引サイト（ショッピングサイト）を対象に、セキュリティ上の注意点をまとめ、公表しました。

“消費者向け電子商取引サイトの運用における注意点”（2005 年 3 月 4 日公表）
http://www.ipa.go.jp/security/vuln/documents/2005/EC_Security.pdf

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**

  ウェブアプリケーションを動作させるために、クライアント側の設定を変更する際には、クライアント PC のセキュリティレベルを低下させないよう注意するとともに、その変更が他のウェブアプリケーションに対して悪影響を及ぼすことのないようにしてください。

- **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、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。アンケートページ等に個人情報を入力する際には、通信が暗号化されているかどうか（URL が https://で始まっているか、ブラウザの右下に鍵のマークが表示されているか）を確認してください。暗号化されていない情報は通信路で盗聴される危険性があります。

■ 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

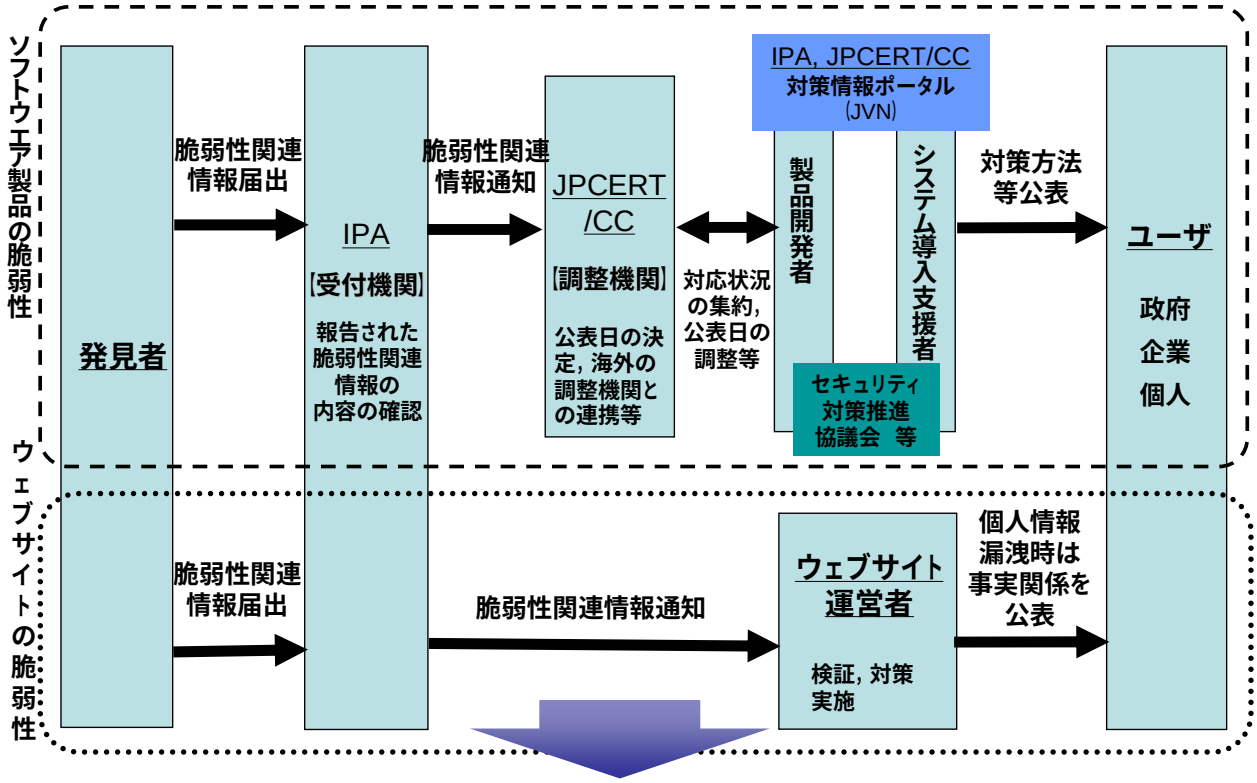
付表 ウェブアプリケーション脆弱性の分類

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
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[11]	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
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	個人情報の漏洩

[11] 4 ページに記載した、Javaアプリケーションの問題が該当します。

脆弱性の種類	深刻度	説明	届出において 想定された脅威
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	本物サイト上の偽情報の表示

「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）