プレスリリース
2006 年 4 月 20 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 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、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、2006 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。

要約

- ソフトウエア製品の脆弱性関連情報

  届出　　：34 件 (届出受付開始からの累計は 167 件)

  脆弱性公表：7 件 (届出受付開始からの累計は 61 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　　：72 件 (届出受付開始からの累計は 507 件)

  修正完了　：32 件 (届出受付開始からの累計は 266 件)

今四半期の特徴は以下の通りです。

ウェブアプリケーションの脆弱性においては、「ファイルの誤った公開」[1]の届出件数が増加しました。これは、複数のウェブサイトで同じショッピングカートを使用しており、設置の際のアクセス権限の設定ミスにより、顧客情報が漏洩しているという届出があったためでした (p.8 図 3-2 参照)。

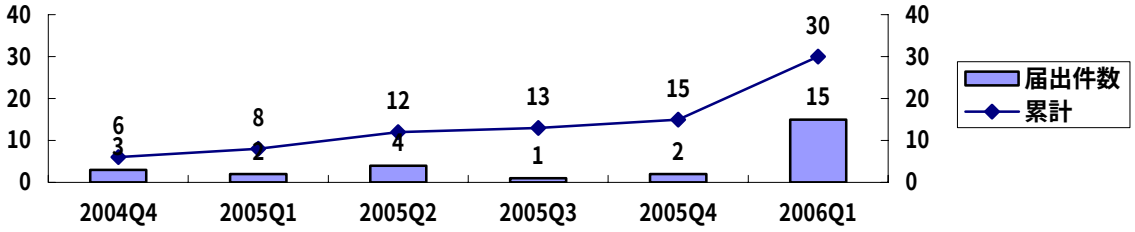


図 「ファイルの誤った公開」の届出件数の推移

ソフトウエア製品の届出においては、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 10 件ありました (p.4 図 2.1 参照)。

[1] 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というものです。

1　届出件数[2]

2006 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、106 件（ソフトウエア製品に関するもの 34 件、ウェブアプリケーションに関するもの 72 件）であり、届出受付開始（2004 年 7 月 8 日）からの累計は 674 件（ソフトウエア製品に関するもの 167 件、ウェブアプリケーションに関するもの 507 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 1.60 件であり、前四半期より増加しています。

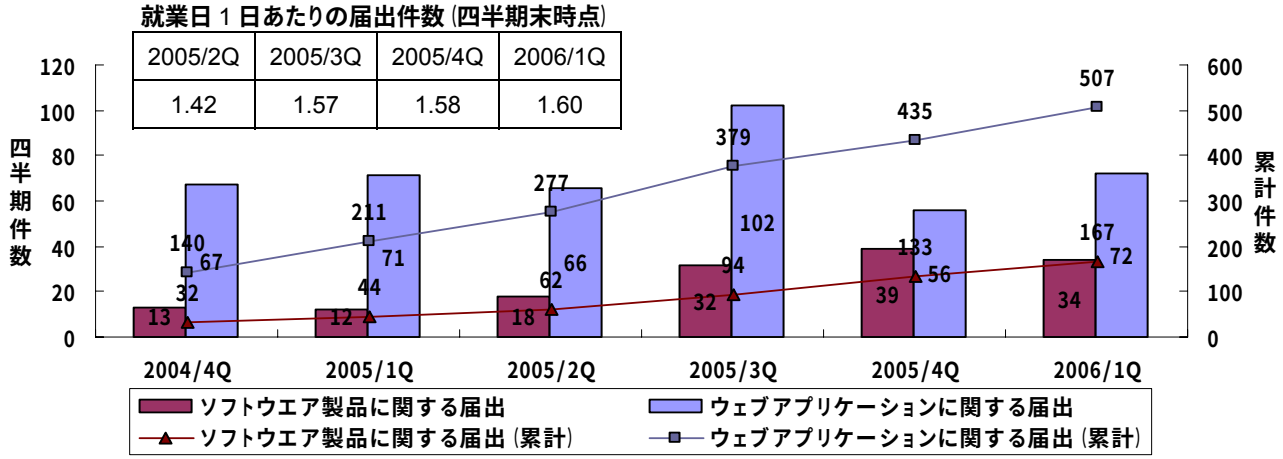


図 1-1 脆弱性関連情報の四半期別届出件数の推移

(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、7 件（累計 61 件）です。また、「不受理」としたものは 7 件（累計 30 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。

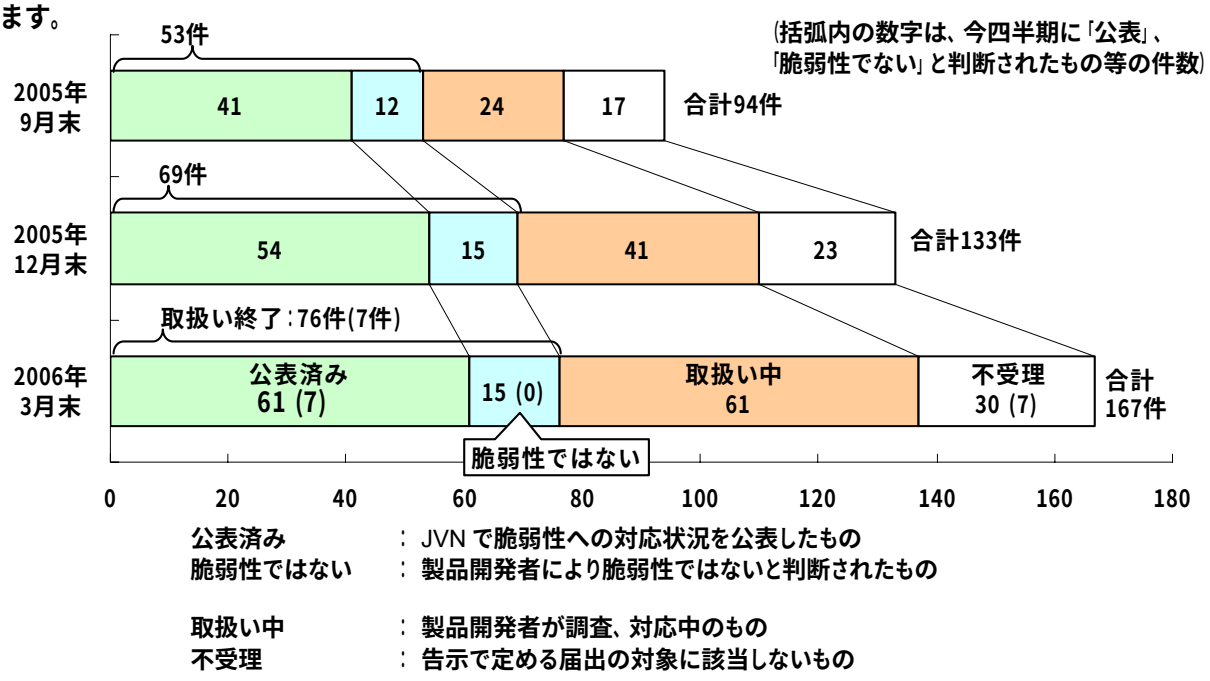


図 1-2 ソフトウエア製品 各時点における脆弱性関連情報の届出の処理状況

[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。

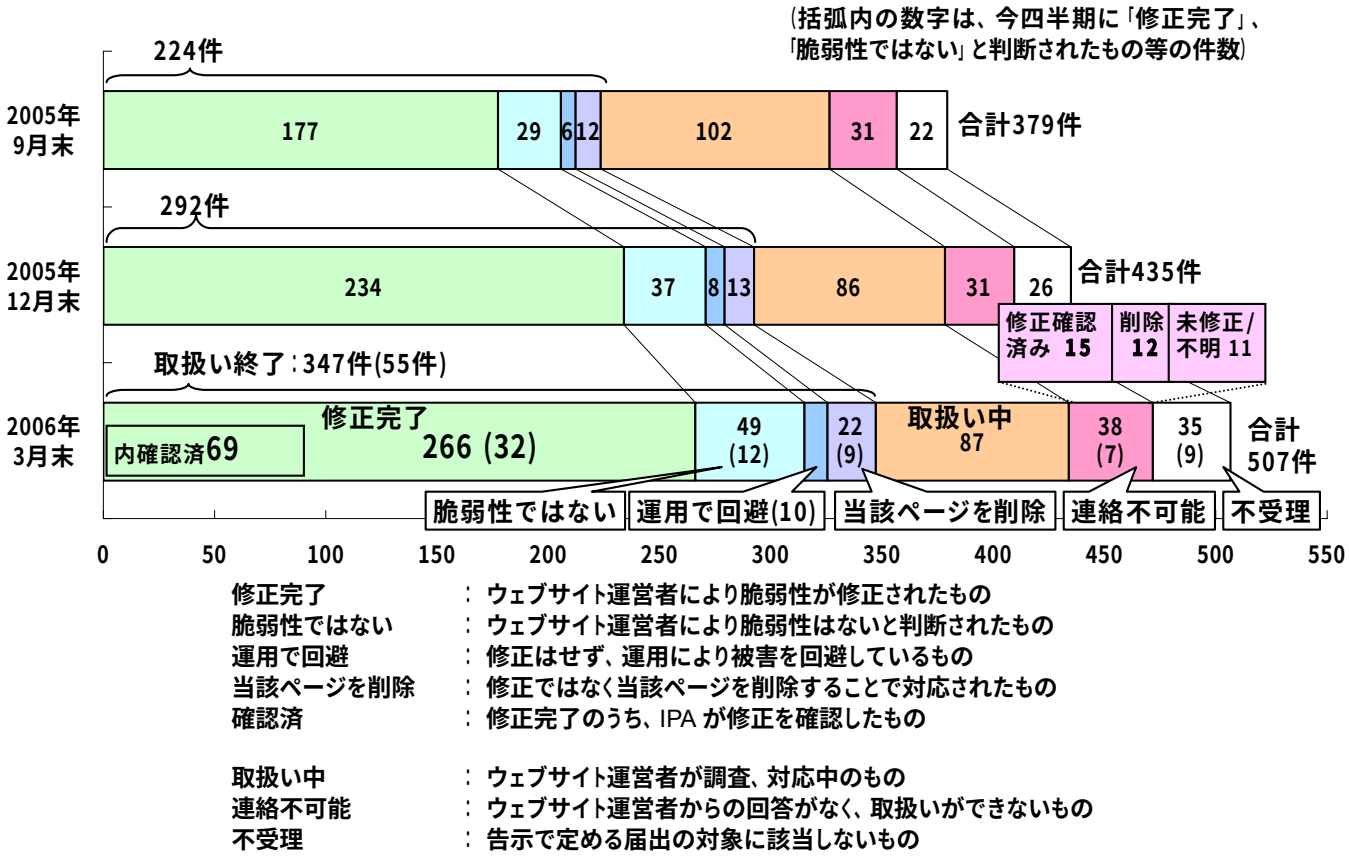
このほかに、製品開発者自身から脆弱性およびその対策情報の連絡を受け、公表したものが 1 件ありました。

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 55 件（累計 347 件）でした。このうち、「修正完了」したものは 32 件（累計 266 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 12 件（累計 49 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 10 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 9 件（累計 22 件）ありました。「修正完了」したもののうちの 1 件（累計 69 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 9 件（累計 35 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 10 件ありました。オープンソースソフトウエアの届出についても、開発者、開発コミュニティに通知し、1 件を除き対応が取られています。これは、既にサポートが終了した機能であるため、新たな修正はしないというものでした。

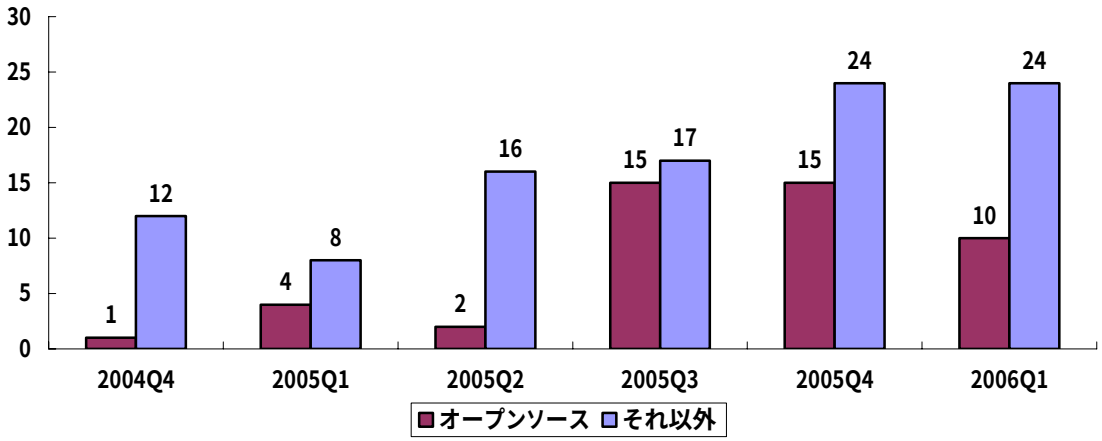
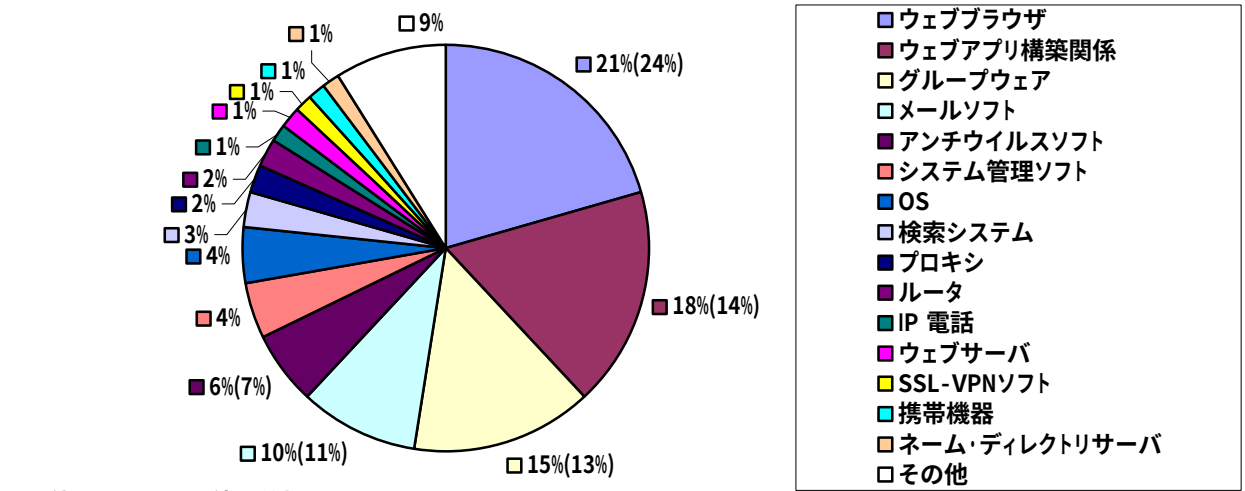


図 2-1　ソフトウエア製品の脆弱性 内訳（届出受付開始から 2006 年 3 月末まで）

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 167 件のうち、不受理のものを除いた 137 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。

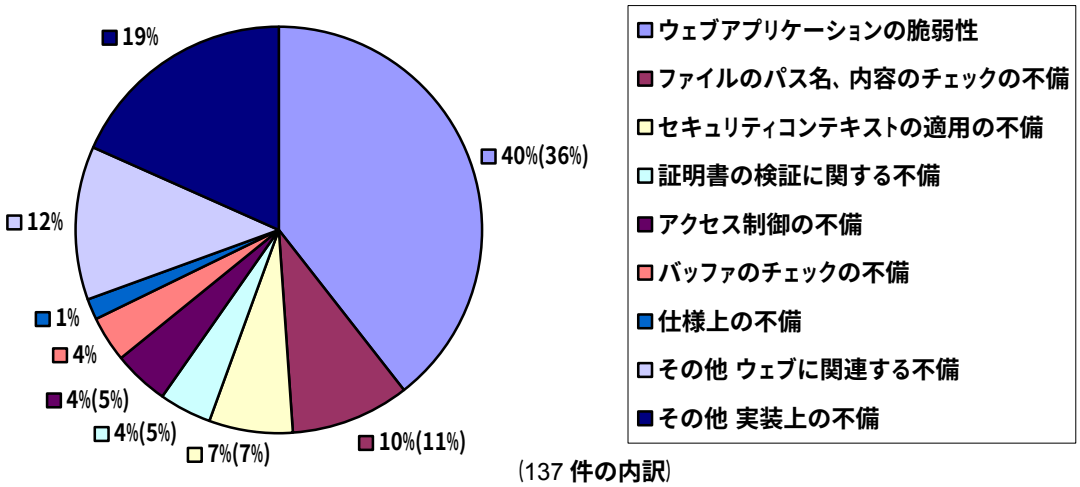


※1 件のものはその他に分類しています。
情報家電、ミドルウェアがあります

（137 件の内訳）　（グラフの括弧内は前四半期の数字）

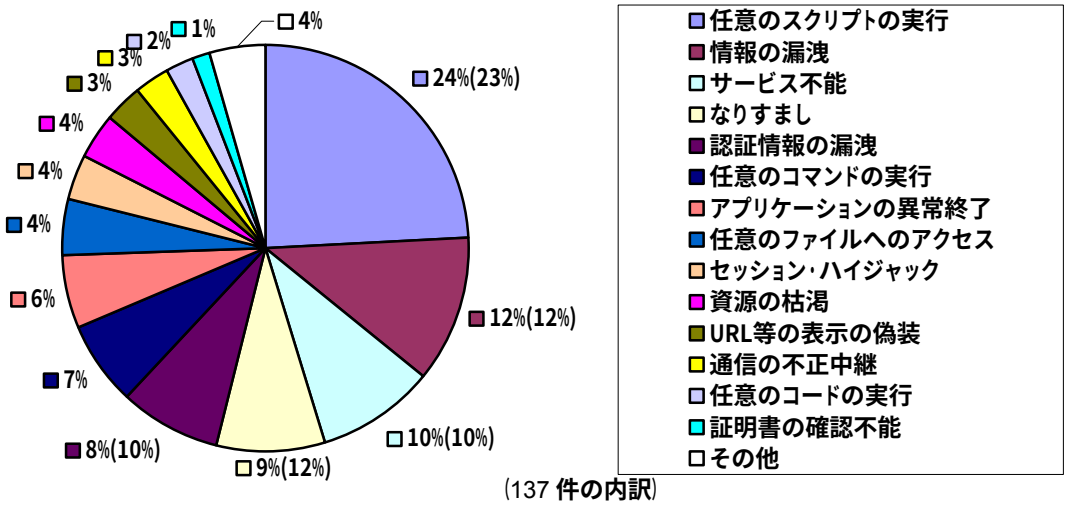
図 2-2　ソフトウエア製品の脆弱性 種類別内訳（届出受付開始から 2006 年 3 月末まで）

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。



(137 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 2006 年 3 月末まで) [3]



(137 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 2006 年 3 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。

今期は、複数のメールクライアントソフトにおいて、2000 年にも問題になった、デバイスファイルの名前を含むファイルの取扱いについての脆弱性 (表 2-2 項番 1) が修正され、公表されました。

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/)。

[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)	7	61
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	6
③	海外 CSIRT から連絡を受けたもの	7	99
	計	15	166

(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 3 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 43%の届出が 45 日以内に公表されています。

平均公表日数

	2005/4Q まで	2006/1Q
当該期公表分	-	114
通算	72	77

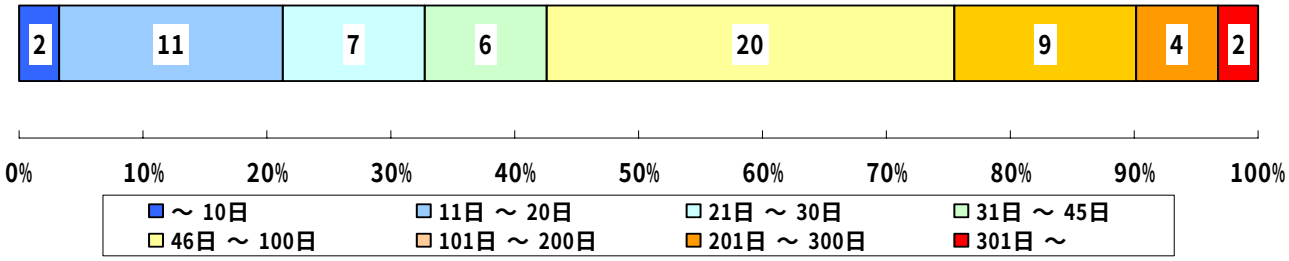


図 2-5 ソフトウエア製品の脆弱性 公表日数

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、2006 年第 1 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、≪複数のメールクライアントソフトにおける、添付ファイルによりメールクライアントソフトが使用不能になる脆弱性≫ (表 2-2 項番 1) の 1 件であり、特定の製品に関する脆弱性は 7 件でした。≪「ハイパー日記システム」においてメールの不正送信が可能な脆弱性≫ (項番 7) 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)。

表 2-2 2006 年第 1 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	複数のメールクライアントソフトにおける、添付ファイルによりメールクライアントソフトが使用不能になる脆弱性	複数のメールクライアントソフトにおいて、添付ファイル名にデバイスファイルの名前を含むメールを取り扱う際に、処理が停止する問題があります。また、停止しないまでも送受信処理が終了しなくなったり、関連付けられたアプリケーションでエラーメッセージが表示される可能性があります。	2006 年 1 月 31 日
特定製品の脆弱性	2	「長崎県電子県庁システム」における認証情報に関する脆弱性	「長崎県電子県庁システム」の一部には、認証情報がソースコード中に組込まれています。ソースコードが公開されているため、第三者が正規ユーザになりすます可能性があります。	2006 年 1 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
特定製品の脆弱性（続き）	3	「長崎県電子県庁システム」における認証処理に関する脆弱性	「長崎県電子県庁システム」の一部には、認証が十分に行われない問題があります。このため、第三者が正規ユーザになりすます可能性があります。	2006 年 1 月 12 日
	4	「Eudora」日本語版が使用できなくなる脆弱性	メールクライアントソフトウェア「Eudora」の日本語版には、破損した画像ファイルを含むメールを表示すると、処理が停止し使用できなくなる問題があります。	2006 年 1 月 17 日
	5	「はてなツールバー」における URL 情報の扱いに関する問題	「はてなツールバー」には、利用者が閲覧しているウェブページの URL 情報を「はてなサーバ」に送信する機能がありますが、この際、URL 中にセッション管理情報などの機密情報が含まれていても、通信を暗号化せずに送信してしまう問題があります。	2006 年 2 月 1 日
	6	「長崎県電子県庁システム」における SQL インジェクションの脆弱性	「長崎県電子県庁システム」の一部には、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 2 月 3 日
	7	「ハイパー日記システム」においてメールの不正送信が可能な脆弱性	「ハイパー日記システム」に同梱されているメッセージ送信プログラムには、日記読者から、細工された入力値を受け取った際に、日記管理者があらかじめ設定したメールアドレス以外の宛先に、メールを送信してしまう問題があります。	2006 年 2 月 28 日
	8	「the Minnu's filer2」において、使用中のユーザの権限で別のユーザに任意の Ruby スクリプトを実行される脆弱性	Unix 用のファイル管理ソフト「the Minnu's filer2」は、処理に利用する Unix ソケットが誰からでもアクセス可能なために、ログイン中の別のユーザにより当該製品を起動中のユーザの権限で任意の Ruby スクリプトが実行されてしまう問題があります。	2006 年 3 月 1 日

⑵ 海外 CSIRT から連絡を受け公表した脆弱性

表 2-3 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。2006 年第 1 四半期は、米国 CERT/CC から 7 件の脆弱性関連情報の連絡を受けました。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。このほか、12 件の US-CERT Technical Cyber Security Alert を JVN で公表しました。

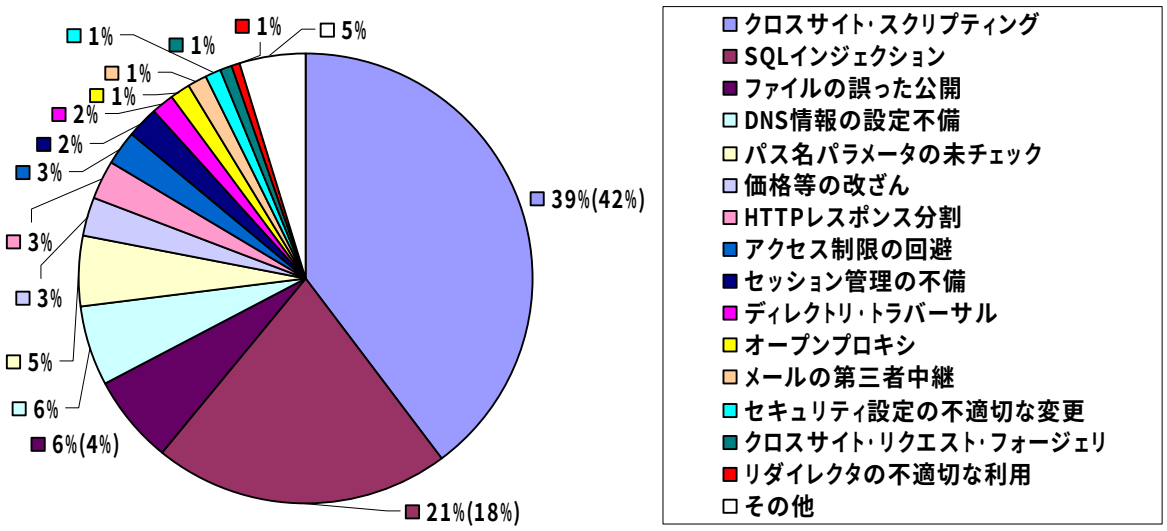
表 2-3 CERT/CC から連絡を受けた脆弱性関連情報および対応状況

項番	脆 弱 性	対応状況
1	Windows メタファイルハンドラで呼び出される GDI Escape ファンクションに脆弱性	JVN 掲載
2	PAM-MySQL にサービス運用妨害 (DoS) 攻撃を受ける脆弱性	JVN 掲載
3	Internet Explorer に ActiveX Control の Kill bit 確認を回避できる脆弱性	JVN 掲載
4	Microsoft Windows の権限昇格に関する脆弱性	複数製品開発者に展開
5	Oracle PL/SQL Gateway の HTTP request 検証機構に脆弱性	JVN 掲載
6	sendmail におけるシグナルの扱いに関する脆弱性	複数製品開発者に展開
7	Microsoft Internet Explorer の createTextRange() に関する脆弱性	JVN 掲載

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507件のうち、不受理のものを除いた472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。



(472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2006年3月末まで)[3]

図 3-1 に示すように、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」が最多ですが、「SQLインジェクション」、「ファイルの誤った公開」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64件のうち、38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26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。

「ファイルの誤った公開」の増加は、複数のウェブサイトで、ショッピングカートを設置する際にアクセス制限の設定に不備があり、利用者の情報が誰からでも閲覧できる状態になってしまっていたという届出があったことによるものです。現在は、利用者の情報にはアクセスできないようになっています。「ファイルの誤った公開」の届出件数の推移を図3-2に示します。

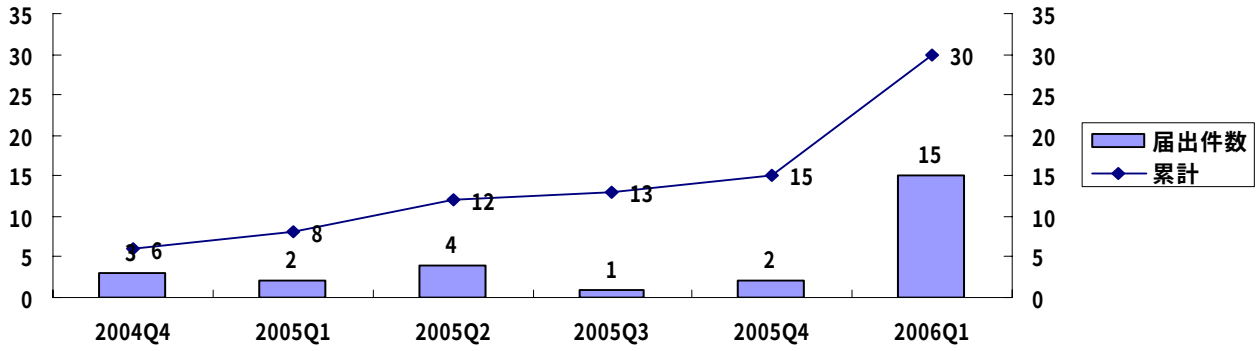
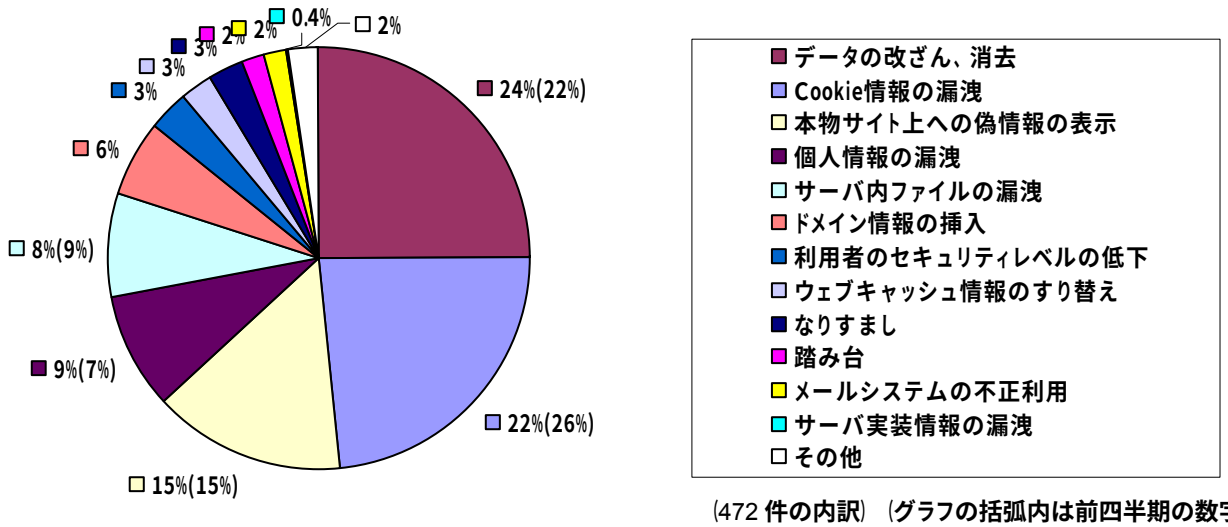


図 3-2　「ファイルの誤った公開」の届出件数の推移



(472 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 3 月末まで)

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「Cookie 情報の漏洩」「本物サイト上への偽情報の表示」があります。また「ファイルの誤った公開」により起こりうる「個人情報の漏洩」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 2006 年 3 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 81%の届出が、90 日以内に修正されています。

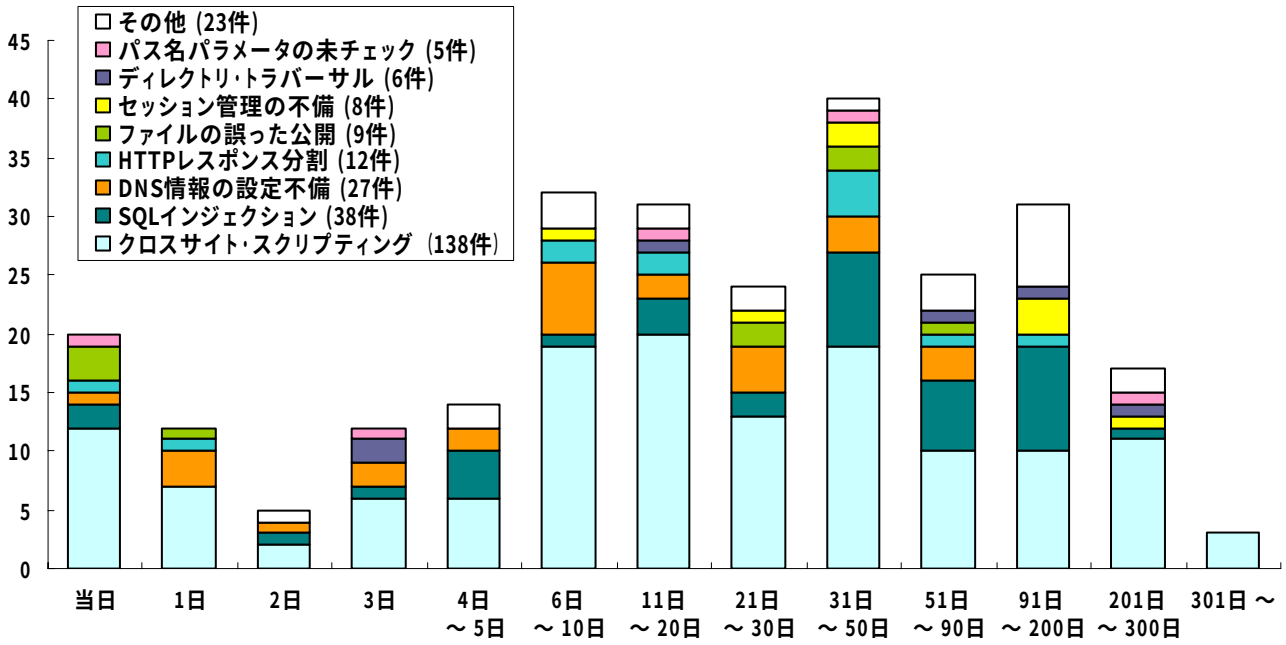


図 3-4 ウェブアプリケーションの脆弱性修正に要した日数

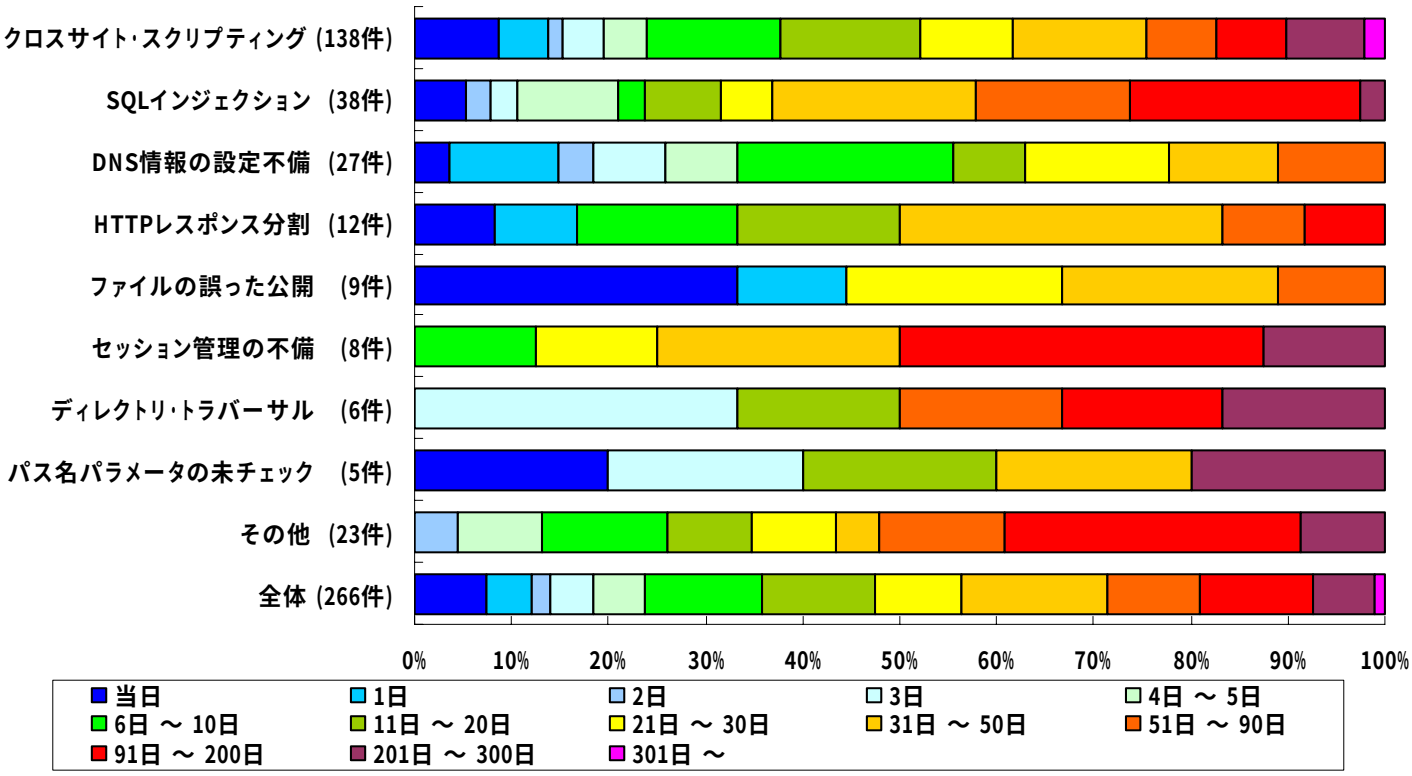


図 3-5　ウェブアプリケーションの脆弱性修正に要した日数の傾向

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およびシステム構築事業者の皆様へ**

  ショッピングカート、メール送信フォームなど、他の人が作成したソフトをダウンロード等で入手し、利用するケースは多いと考えられますが、その利用に際し、そのソフトに脆弱性があったり、設定のミスが原因で、脆弱性が発生しているケースがあります。他の人が作成したソフトを利用する際には、その安全性を充分に確認してください。

- **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。

■ 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 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	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

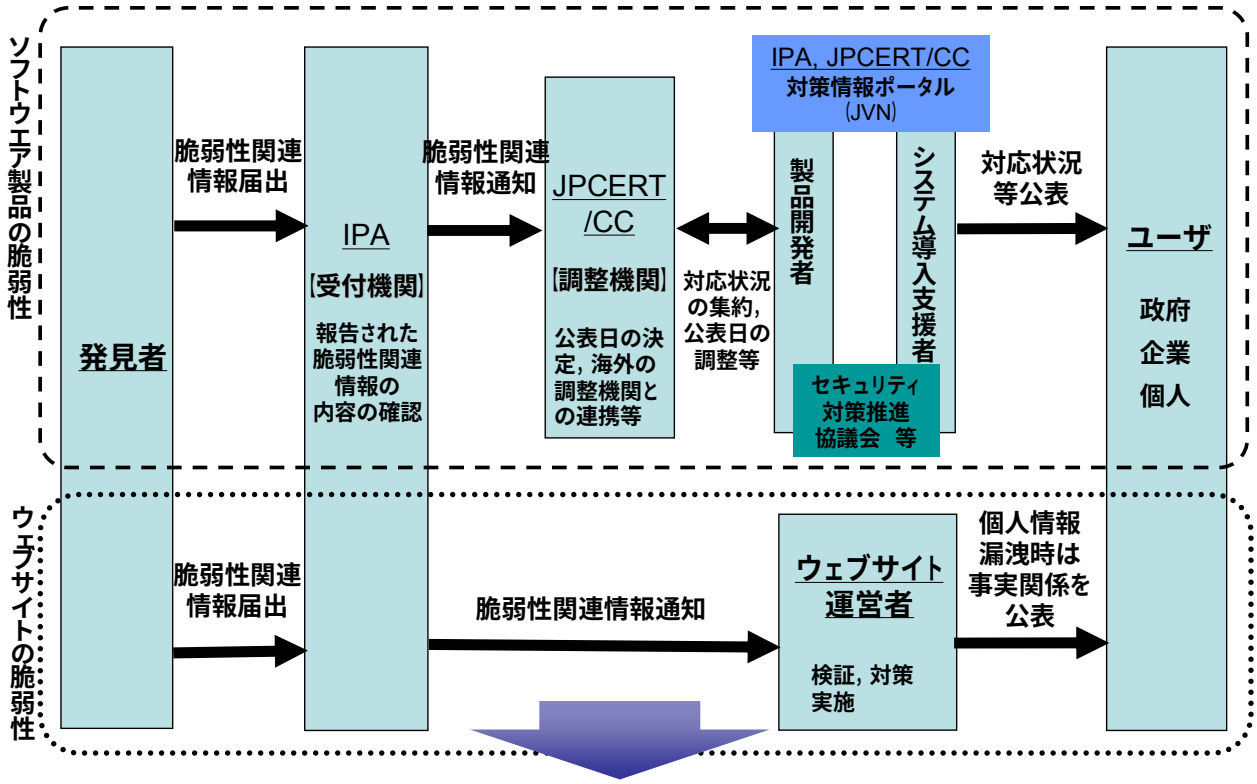
付表 2 ウェブアプリケーション脆弱性の分類

	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	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	個人情報の漏洩 なりすまし 利用者のセキュリティレベルの低下
8	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
9	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
10	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
11	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
12	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
13	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
14	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	メールシステムの不正利用
15	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
16	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
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

「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