IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

プレスリリース
2004 年 10 月 18 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 [2004 年第 3 四半期 (7 月～9 月)]

独立行政法人 情報処理推進機構 (略称：IPA) 及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 年第 3 四半期 (7 月～9 月) の脆弱性関連情報届出状況を、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、IPA は 2004 年 7 月 8 日より脆弱性関連情報の届出の受付を開始し、JPCERT/CC は日本国内の製品開発者などの関連組織との調整を行いました。ソフトウエア製品の脆弱性については、19 件の届出のうち、3 件について製品開発者による対策が完了し、公表されました。このうちの 1 件は、JPCERT/CC が海外 CSIRT[1]と連携し、海外の製品開発者も含めて調整をしたものです。ウェブアプリケーションの脆弱性については、73 件の届出のうち、10 件について修正が完了しました。

1. 届出件数

2004 年 7 月 8 日から 9 月 30 日までの IPA への脆弱性関連情報の届出件数は、総計 92 件 (ソフトウエア製品に関するもの 19 件、ウェブアプリケーションに関するもの 73 件) でした。月別の届出状況を表 1-1 に示します。

表 1-1 脆弱性関連情報の月別の届出状況

	2004 年 7 月	2004 年 8 月	2004 年 9 月	合計
ソフトウエア製品に関する届出	7	7	5	19
ウェブアプリケーションに関する届出	17	36	20	73
合計	24	43	25	92

(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については、対策を終了し公表されたものが 3 件、製品開発者により脆弱性ではないと判断されたものが 1 件あります。また、告示で定める届出の対象に該当せず、取扱い対象外としたものが 3 件あります。この 3 件の内訳は、製品の仕様であり脆弱性ではないと判断されたものが 2 件、届出時に公知の情報だったものが 1 件となっています。

(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については、修正を完了したものが 10 件、脆弱性を運用で回避したものが 4 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が 5 件あります。取扱い対象外としたものの内訳は、届出時に既に修正済みであったものが 1 件、日本国内からのアクセスを想定したウェブサイトでないものであったものが 3 件でした。このほか、16 件が、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 (取扱い不能) となっています。

[1] Computer Security Incident Response Team の略であり、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。

届出の取扱い状況を図 1-1 に示します。

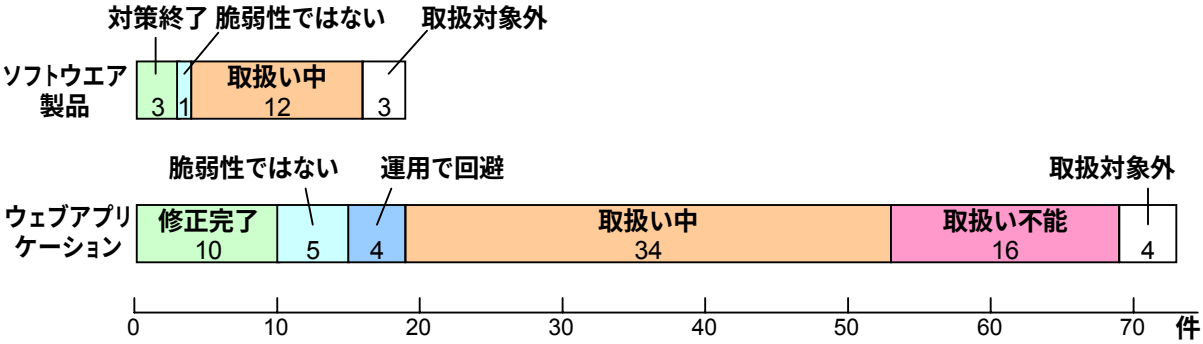

図 1-1 脆弱性関連情報の届出の取扱い状況

2. ソフトウエア製品の脆弱性関連情報の届出

JPCERT/CC が日本国内の製品開発者などの関連組織との調整を行ない、公表した脆弱性関連情報は 7 件です。このうち、IPA への届出により手続きを開始した脆弱性関連情報は 3 件であり、そのうちの 1 件である「SSL-VPN 製品における Cookie の脆弱性」については、海外 CSIRT とのパートナーシップに基づき、海外開発者も含めて調整しました。これは、企業内システムを社員が外出先からインターネット経由で利用できるようにする VPN (Virtual Private Network)を、従来よりも手軽に実現するものとして近年注目を浴びてきた「SSL-VPN」製品に対し、その使い方によっては、必ずしも VPN ほどの堅牢な安全性が確保されるとは限らないことが指摘されたものです。一部の製品には、一般的なウェブアプリケーションにみられる脆弱性と同種の欠陥を有するものがあり、パケット盗聴によるセッションハイジャック攻撃を許してしまうものがありました。

他の 4 件は、海外 CSIRT からの脆弱性情報について JPCERT/CC が日本国内の製品開発者との調整を行ったものです。

製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している対策情報ポータルサイトである JP Vendor status Notes (JVN) において公開しています。(URL：http://jvn.jp/)

表 2-1 に、IPA に届出があり、対策が完了し公表した脆弱性を示します。

取扱い対象の届出 16 件のうち、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の届出は 2 件あり、これらは、JPCERT/CC が複数の製品開発者に対して調整を行いました。特定製品の脆弱性関連情報の届出は 14 件であり、アンチウイルスソフトやメールソフトなどのクライアント製品が多くありました。また、情報家電において、アクセス制御機能が適切に機能していない問題も 1 件ありました。特定製品の脆弱性の製品種類別の内訳を図 2-1 に示します。

表 2-1 対策が完了した届出

	種類	脆弱性の概要	JVN 公表日
1	SSL-VPN 製品における Cookie の脆弱性	SSL-VPN 製品について、SSL のクライアント認証を使用せずに、ユーザ名とパスワードでログインするモードを使用している場合に、Cookie 情報が漏洩し、セッションハイジャックされる可能性があります。これは、複数製品に関わる脆弱性であり、海外製品開発者も含めて調整されました。	2004 年 9 月 30 日
2	desknet's の脆弱性	株式会社ネオジャパンのウェブグループウェアである desknet's に関して、ユーザが悪意のあるスクリプトを含んだ HTML メールやインフォメーション（掲示板に相当する機能）を参照した場合に、スクリプトが実行されます。結果として、Cookie 情報（設定によっては ID やパスワードを含む）の漏洩によるなりすましや個人情報の漏洩などが発生する可能性があります。	2004 年 9 月 24 日
3	ウィルスバスターコーポレートエディションの脆弱性	トレンドマイクロ株式会社の企業向け総合セキュリティ対策ソフトウエアであるウィルスバスターコーポレートエディションに関して、管理コンソールに問題があり、特定の URL を指定すると OPP.ini ファイル(Outbreak Prevent Policy の設定ファイル)を閲覧できます。	2004 年 9 月 3 日

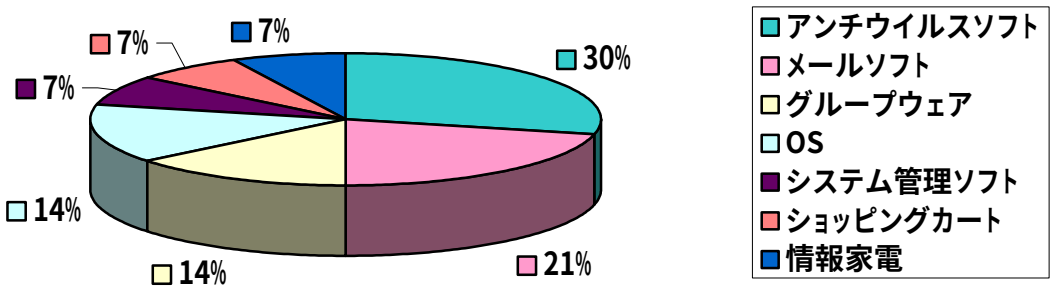

図 2-1　ソフトウエア製品種類別の届出内訳

3. ウェブアプリケーションの脆弱性関連情報の届出

ウェブアプリケーションについては、19 件の届出について取扱い終了しました。内訳としては、修正を完了したものが 10 件、脆弱性を運用で回避しているものが 4 件、ウェブサイト運営者により脆弱性が存在しないと判断されたものが 5 件です。修正や回避等により、最終的に脆弱性に対処したものは 19 件中 14 件ですが、取扱い中のものにも、修正完了の報告を受け IPA による修正確認中のものが 4 件あります。

修正された届出の脆弱性の種類別の修正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 脆弱性の種類別の修正件数および修正日数

脆弱性	件数	修正日数
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）	9	平均 15 日
パス名パラメータの未チェック（フォーム入力値の改ざん）	3	当日、3 日、16 日
ファイルの誤った公開	1	21 日
SQL インジェクション（データベースへの不正な入力）	1	39 日

脆弱性の種類別内訳を図 3-1 に、想定される脅威別内訳を図 3-2 に示します。脆弱性の種類は、「クロスサイト・スクリプティング[2]」が最も多く、ユーザからの入力を十分にチェックしていないウェブサイトが多いことがわかります。次いで「パス名パラメータの未チェック」が多くなっていますが、これは、あるウェブアプリケーション部品が多くのウェブサイトで使用されていたことによります。

脆弱性から想定される脅威は、「サーバ内ファイルの漏洩」が最も多く、次いで「Cookie[3]情報の漏洩」でした。利用者の識別に Cookie 情報が使われている場合には、Cookie 情報の漏洩により、なりすましや個人情報漏洩につながる可能性があります。また、ファイルの誤った公開の脆弱性がある場合には、多数の個人情報が一度に漏洩する可能性がありますし、セッション管理の不備の脆弱性がある場合には、個人情報などを含む Web ページが第三者に閲覧されてしまう可能性があります。

実際に、修正が完了した 2 件のウェブサイトからも、個人情報が漏洩する可能性があった、との報告がありました。

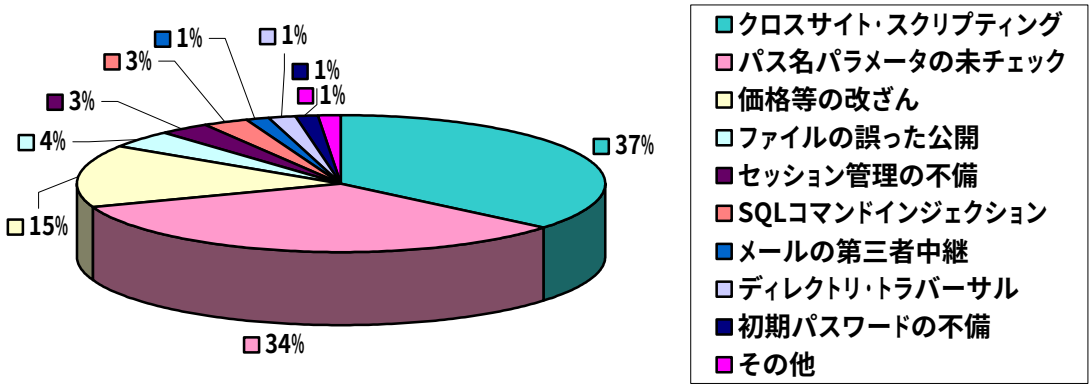

図 3-1　ウェブアプリケーションに関する脆弱性関連情報の届出の種類別内訳

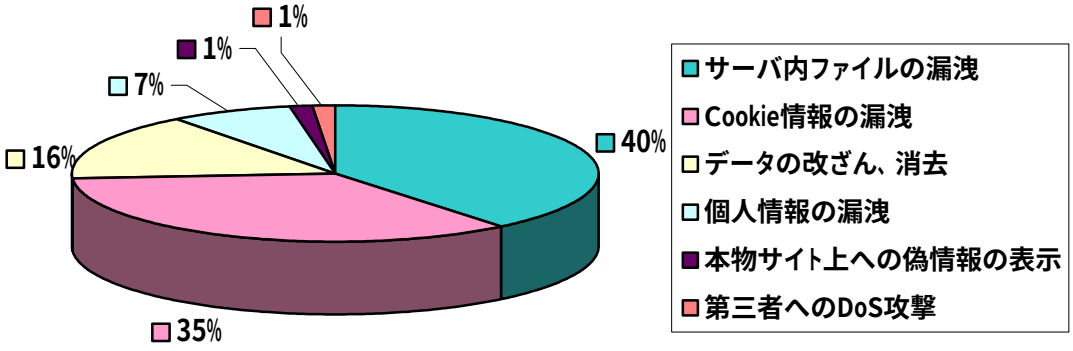

図 3-2　ウェブアプリケーションに関する脆弱性関連情報の届出の脅威別内訳

[2] 脆弱性の説明については付録を参照してください。

[3] 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。

4. 皆様へのお願い

届出の受付開始から約3ヶ月が経過しましたが、脆弱性の修正をより強く促進していくために、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の皆様へ**

  ウェブアプリケーションの作成にあたっては、入力フォーム等へのユーザからの入力に対してスクリプトや命令が含まれていないか、想定外のパス名が与えられる可能性がないかを十分にチェックするか、もしくは適切なエスケープ処理を施すように設計してください。

  IPA からの連絡はウェブサイトに記載のある窓口に対して、電子メールまたは電話で行っています。本制度の趣旨をご理解のうえ、窓口の明確化および連絡があった場合のご協力をお願いします。IPA からの連絡について、本当に IPA からの連絡かどうか等の疑問を感じられた場合は、メール (vuln-inq@ipa.go.jp) もしくは電話 (03-5978-7527) にて、ご連絡ください。

- **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/)

- **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。

■ 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
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	パス名（ファイル名）を指定するCGIパラメータに、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相対的にアクセスできる	サーバ内ファイルの漏洩
セッション管理の不備	高	セッション管理用のパラメータにおいて、秘密情報が含まれておらず、容易に予測ができる	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、実行させることができる	サーバ内ファイルの漏洩 データの改ざん、消去
クロスサイト・スクリプティング	中	悪意のあるスクリプトをウェブサイトへの入力中に記述し、第三者に対し悪意のある行為を仕掛けることができる	Cookie情報の漏洩 本物サイト上への偽情報の表示
メールの第三者中継	低	他人のメールサーバを用いて、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
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改ざんできる	データの改ざん、消去