IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT CC

プレスリリース
2005 年 10 月 12 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 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) 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 3 四半期 (7 月～9 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　　：32 件 (届出受付開始からの累計は 94 件)
  脆弱性公表：12 件 (届出受付開始からの累計は 41 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 2 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　　：102 件 (届出受付開始からの累計は 379 件)
  修正完了　：53 件 (届出受付開始からの累計は 177 件)

1　届出件数[1]

2005 年 7 月 1 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、134 件 (ソフトウエア製品に関するもの 32 件、ウェブアプリケーションに関するもの 102 件) であり、届出受付開始 (2004 年 7 月 8 日) からの累計は 473 件 (ソフトウエア製品に関するもの 94 件、ウェブアプリケーションに関するもの 379 件) です。四半期毎の届出状況を図 1-1 に示します。

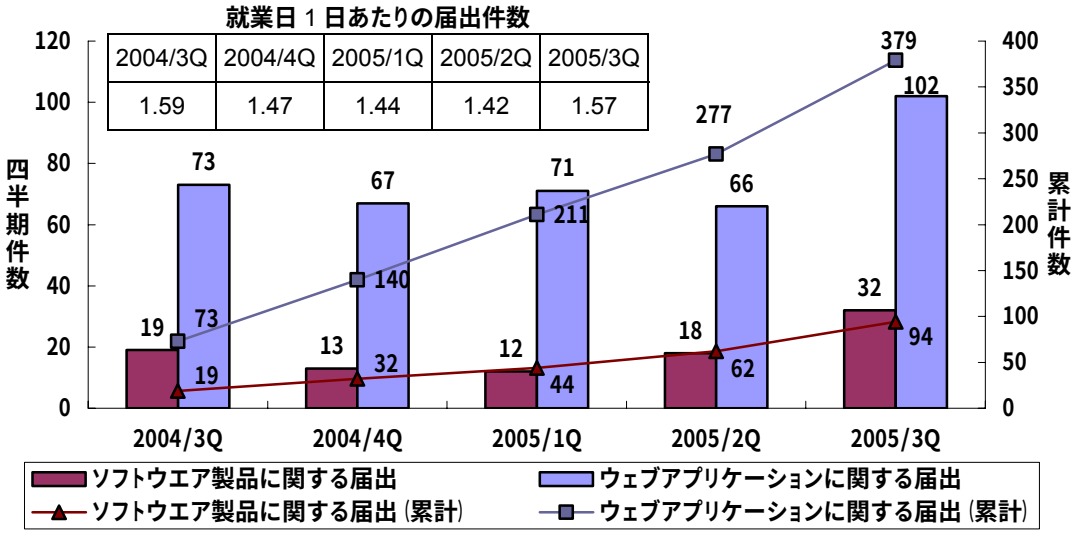


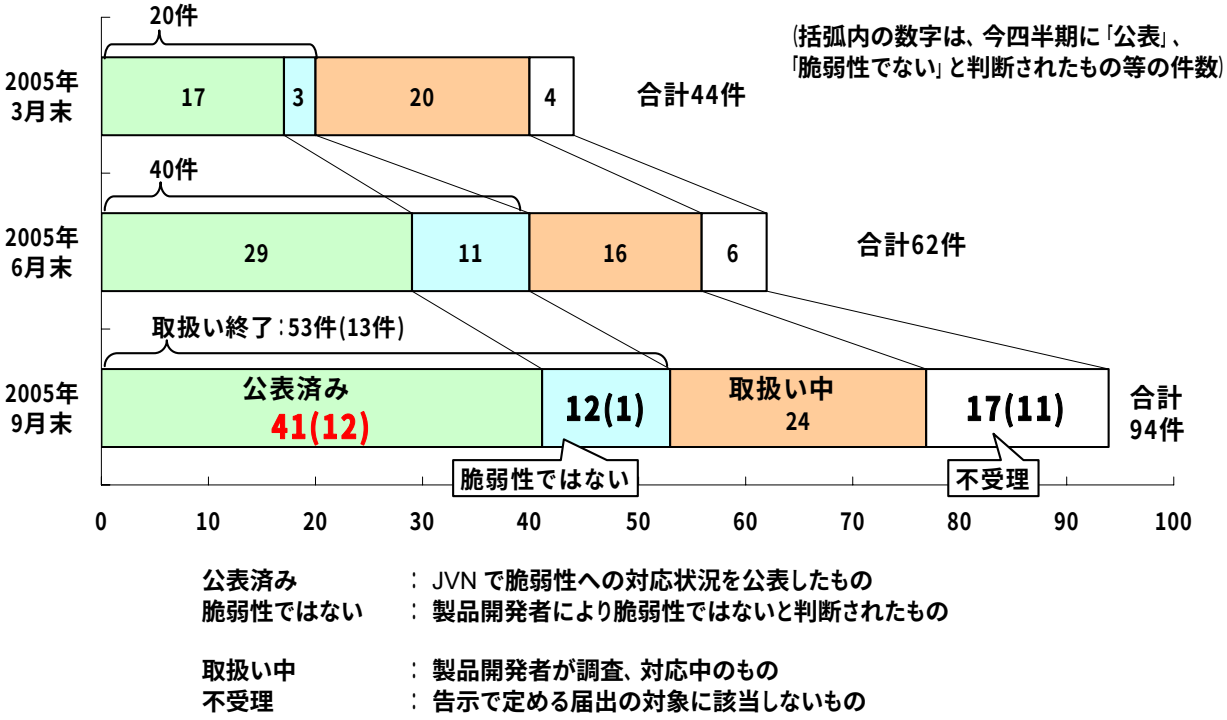
図 1-1 脆弱性関連情報の四半期別届出件数の推移

[1] 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

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[2]した脆弱性は、**12** 件 (累計 **41** 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 1 件 (累計 12 件)、「不受理」としたものは 11 件 (累計 17 件) ありました。不受理にしたものの中には、製品の不具合ではあるものの悪用のシナリオが想定できず、セキュリティ上の問題とはいえないものも 4 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

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 2 件ありました。

(2) ウェブアプリケーションの脆弱性

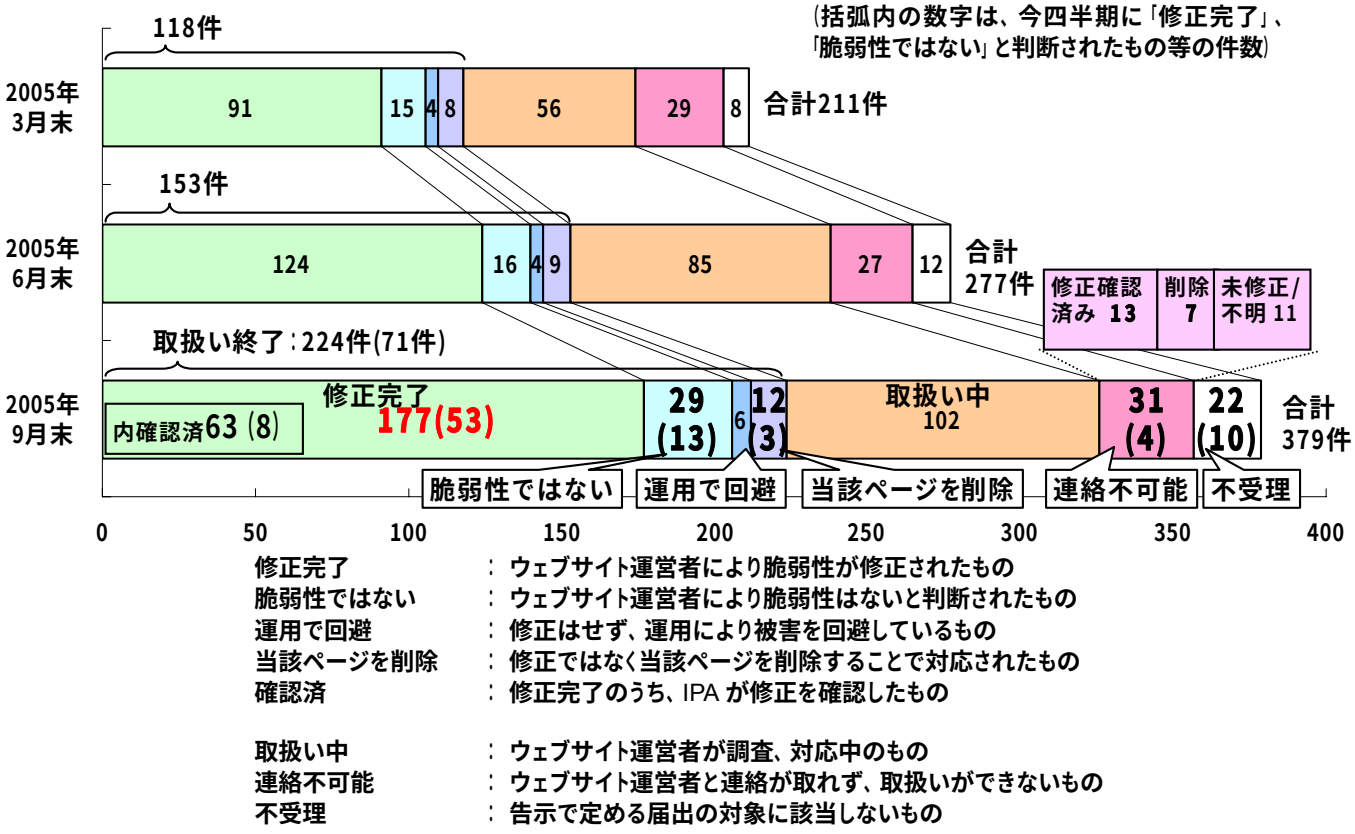
ウェブアプリケーションの脆弱性関連情報の届出について、処理状況を図 1-3 に示します。

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 71 件 (累計 224 件) でした。このうち、「修正完了」したものは **53** 件 (累計 **177** 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 13 件 (累計 29 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 3 件 (累計 12 件) ありました。「修正完了」したもののうち 8 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 (累計 63 件)、そのうち 1 件で、修正が不十分なために見直しを依頼しました。

---

[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。

このほか、「連絡不可能」（ウェブサイト運営者と連絡が取れず、処理できない状態）になったものが 4 件（累計 31 件）、「不受理」としたものが 10 件（累計 22 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、郵送手段を用いるなどして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

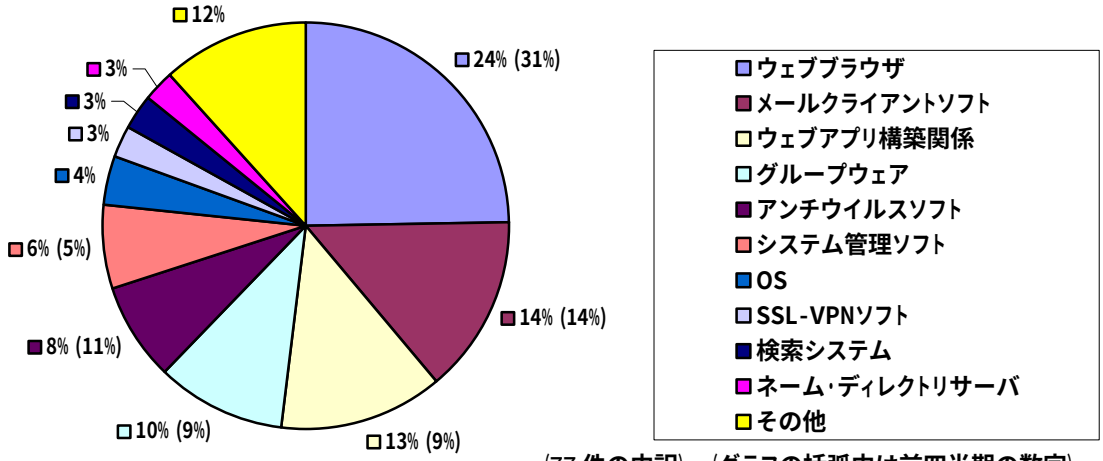
取扱い中　：ウェブサイト運営者が調査、対応中のもの
連絡不可能　：ウェブサイト運営者と連絡が取れず、取扱いができないもの
不受理　：告示で定める届出の対象に該当しないもの

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

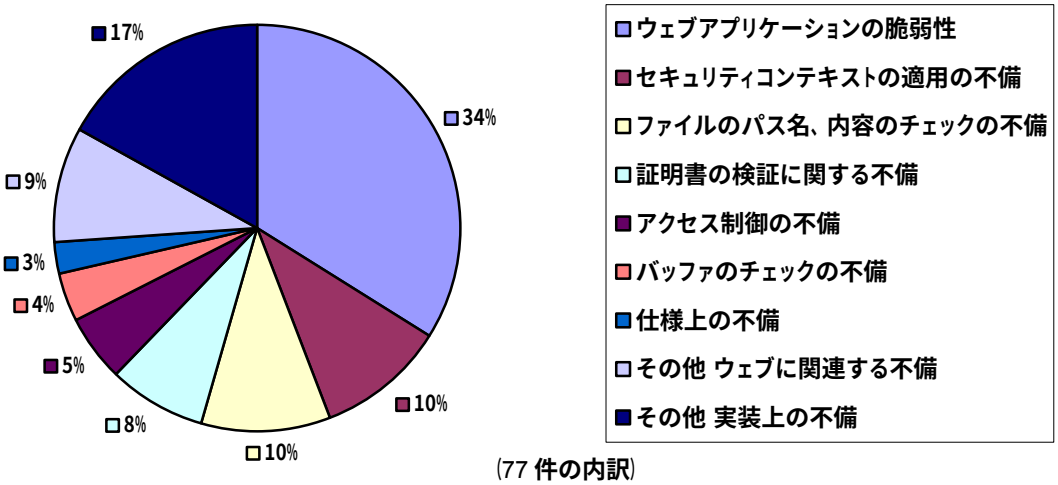
届出受付開始から今四半期までに IPA に届出られたソフトウエア製品に関する脆弱性関連情報 94 件のうち、不受理のものを除いた 77 件の製品種類別の内訳を図 2-1 に、原因別の内訳を図 2-2 に、脅威別の内訳を図 2-3 に示します。



(77 件の内訳)　(グラフの括弧内は前四半期の数字)

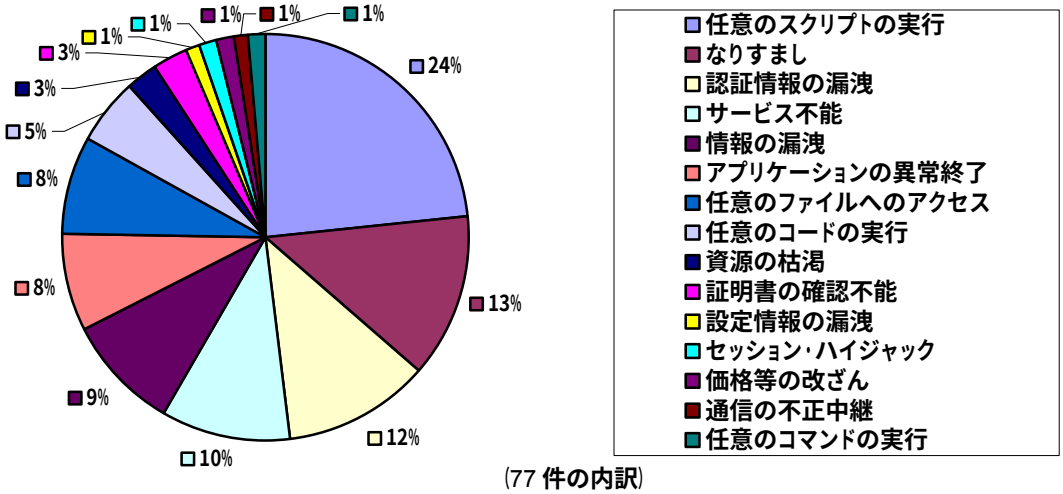
※1 件のものはその他に分類しています。
ウェブサーバ、プロキシサーバ、情報家電、携帯機器、ルータがあります

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 9 月末まで)



(77 件の内訳)

図 2-2　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 9 月末まで) [3]



(77 件の内訳)

図 2-3　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 9 月末まで)

[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。

図 2-1 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。図 2-2 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 2-3 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。

ウェブアプリケーションの脆弱性以外に、本来実行すべき権限よりも高い権限で処理を実行してしまう「セキュリティコンテキストの適用の不備」、処理の際に利用するファイルのパス名や内容のチェックが十分でないために問題が発生する「ファイルのパス名、内容のチェックの不備」が多くありました。

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/)。

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	41
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	2	4
③	海外 CSIRT から連絡を受けたもの	24	81
	計	38	126

(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 39 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 74 日となりました。

表 2-2 ソフトウエア製品の脆弱性 平均公表日数

	2004/2Q	2004/3Q	2004/4Q	2005/1Q	2005/2Q
当該期公表分	49	43	101 [5]	115 [5]	39
通算	49	45	71 [5]	88 [5]	74

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 3 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、≪Internet Explorer コンポーネントを使用するアプリケーションにおけるセキュリティゾーンの扱いに関する脆弱性≫ (表 2-3 項番 1)、≪複数のウェブブラウザにおいてリクエスト分割が可能な脆弱性≫ (項番 2)、≪「Tomcat」におけるリクエスト処理に関する脆弱性≫ (項番 3) の 3 件であり、特定の製品に関する脆弱性は 11 件でした。≪「Common Management Agent」3.x における情報漏えいの脆弱性≫ (項番 7)、≪「WirelessIP5000」における複数の脆弱性≫ (項番 14) 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、≪「Java Cryptography Extension 1.2.1 (JCE 1.2.1)」の証明書の期限切れで

[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] 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。

2005/07/28 以降ソフトウエアが正常に動作しなくなる問題≫ (項番 15) は、脆弱性ではありませんが多くの製品に影響することが考えられたため、ユーザへの周知を目的として、製品開発者の対応状況を取りまとめ、JVN で公開しました。

表 2-3 2005 年第 3 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	Internet Explorer コンポーネントを使用するアプリケーションにおけるセキュリティゾーンの扱いに関する脆弱性	Microsoft Internet Explorer では、ウェブコンテンツが置かれているゾーン(インターネット、イントラネットなど)ごとにセキュリティ設定を適用し、閲覧の際に、厳しいセキュリティ制限をかけることができます。IE の機能を利用する一部の製品は、インターネットゾーンで表示すべきウェブコンテンツを、インターネットゾーンよりもセキュリティ制限が緩いゾーンで表示する問題があり、その結果、セキュリティ制限の緩いゾーンで任意のコードが実行される危険性があります。	2005 年 7 月 12 日
	2	複数のウェブブラウザにおいてリクエスト分割が可能な脆弱性	複数のウェブブラウザにおいて、JavaScript で使用できる XmlHttpRequest オブジェクトの処理に脆弱性が確認されました。本来であれば制限されているドメインに対し、ユーザが利用している任意のドメインの認証情報や、Cookie 情報が漏洩する可能性があります。	2005 年 9 月 29 日
	3	「Tomcat」におけるリクエスト処理に関する脆弱性	Java Servlet または Java Server Pages のサーバ実装である Apache Tomcat において、特定の POST リクエストが適切に処理されない脆弱性が確認されました。別のユーザになりすました処理が行われる可能性があります。	2005 年 9 月 30 日
特定製品の脆弱性	4	「tDiary」におけるクロスサイト・リクエスト・フォージェリの脆弱性	ウェブ日記を支援するソフトウエア「tDiary」において、脆弱性が確認されました。日記を書く人が悪意あるページを読み込んだ場合、「tDiary」に意図しない指示を送り、日記本文の変更や削除、「tDiary」 の設定変更、任意のコード実行がされる可能性があります。	2005 年 7 月 21 日
	5	「QRcode Perl CGI & PHP scripts」におけるサービス運用妨害の脆弱性	QR コード画像を作成するための CGI プログラム「QRcode Perl CGI & PHP scripts」において、特定のリクエストにより、CGI プログラムがサーバ上のリソースを過剰に消費してしまう問題が確認されました。	2005 年 7 月 28 日
	6	「Hiki」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「Hiki」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 8 月 4 日
	7	「Common Management Agent」3.x における情報漏えいの脆弱性	「ePolicy Orchestrator」および「ProtectionPilot」で使用されている「Common Management Agent」には、ディレクトリのアクセス権設定に問題があり、ファイル一覧を取得されたり、ファイルを閲覧される可能性があります。	2005 年 8 月 24 日
	8	「Pochy」におけるサービス運用妨害(DoS)の脆弱性	メールクライアントソフトウェア「Pochy」において、ヘッダの日付部分に特定の文字列を含むメールを POP3 プロトコルで受信した場合に、CPU の負荷が高くなり、受信処理が終了しない問題が確認されました。	2005 年 8 月 25 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
	9	「FreeStyle Wiki」におけるコマンド・インジェクションの脆弱性	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「FreeStyle Wiki」において、脆弱性が確認されました。Wiki サイトの管理者権限を持つユーザにより、CGI の実行権限で任意の Perl コマンドを実行される可能性があります。	2005 年 8 月 29 日
	10	「ハイパー日記システム」におけるクロスサイト・リクエスト・フォージェリの脆弱性	ウェブ日記を書くことを支援するソフトウエア「ハイパー日記システム(hns)」において、脆弱性が確認されました。日記を書く人が、悪意あるページを読み込んだ場合、「hns」に意図しない指示を送り、日記本文の新規作成や変更、削除をしてしまう可能性があります。	2005 年 9 月 1 日
	11	「Webmin」および「Usermin」における認証回避の脆弱性	Unix のシステム管理をウェブブラウザから行うためのインターフェース「Webmin」および「Usermin」において、認証を回避される脆弱性が確認されました。遠隔の第三者により、管理者権限で「Webmin」および「Usermin」の機能を悪用される可能性があります。	2005 年 9 月 20 日
	12	「Ruby」においてセーフレベル 4 がサンドボックスとして機能しない脆弱性	オブジェクト指向スクリプト言語「Ruby」において、信頼できないプログラムによるファイルアクセスや OS コマンドの実行などを制限するための「セーフレベル」を回避できる脆弱性が確認されました。本来制限しているはずの操作が実行されてしまう可能性があります。	2005 年 9 月 21 日
	13	「Unicode 版 msearch」におけるクロスサイト・スクリプティングの脆弱性	ウェブページの全文検索機能を提供する CGI プログラム「Unicode 版 msearch」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 9 月 22 日
	14	「WirelessIP5000」における複数の脆弱性	ワイヤレス IP 電話機「WirelessIP5000」において、複数の脆弱性が確認されました。遠隔の第三者により、不正な情報収集や設定変更などが行われる可能性があります。	2005 年 9 月 30 日
その他	15	Java Cryptography Extension 1.2.1 (JCE 1.2.1) の証明書の期限切れで 2005/07/28 以降ソフトウエアが正常に動作しなくなる問題	サン・マイクロシステムズ社が提供する Java 暗号化拡張機能である Java Cryptography Extension 1.2.1 (JCE 1.2.1) で、パッケージの署名に使われている証明書の有効期限が切れた場合に、JCE の一部の機能が動作しなくなります。そのため、JCE を利用した製品の動作に不具合が起きる可能性があります。	2005 年 7 月 13 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。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 3 四半期は、米国 CERT/CC から 24 件、英国 NISCC (National Infrastructure Security Co-ordination Centre) から 2 件の合計 26 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および対応状況

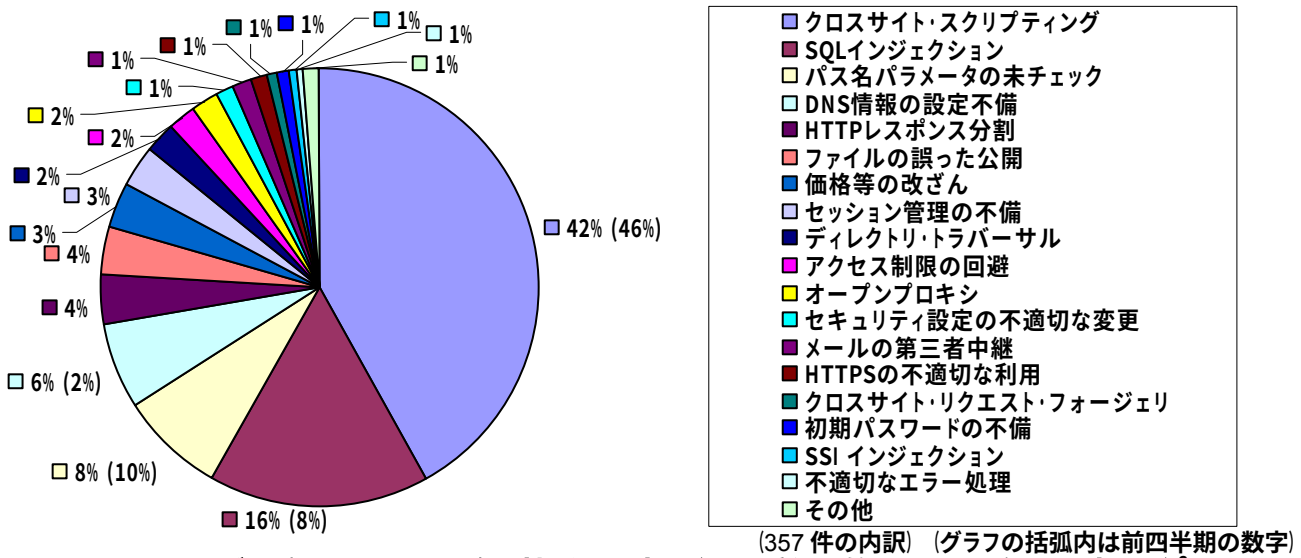
項番	脆 弱 性	対応状況
1	データ圧縮ライブラリ zlib におけるバッファーオーバーフローの脆弱性	複数製品開発者に展開
2	MIT Kerberos5 Key Distribution Center にヒープオーバフローの脆弱性	複数製品開発者に展開
3	MIT Kerberos5 krb5_recvauth()におけるメモリ二重解放の脆弱性	複数製品開発者に展開
4	MIT Kerberos5 Key Distribution Center にメモリのヒープ領域が破壊される脆弱性	複数製品開発者に展開
5	VERITAS Backup Exec Server Service にヒープオーバーフローの脆弱性	複数製品開発者に展開
6	VERITAS Backup Exec に遠隔からレジストリにアクセスされる脆弱性	複数製品開発者に展開
7	Microsoft Windows、Internet Explorer および Word における脆弱性	JVN 掲載
8	Oracle 製品群に複数の脆弱性	JVN 掲載
9	Cisco IOS に IPv6 パケットの処理に関する脆弱性	単独製品開発者に展開
10	Cisco IOS IPv6 に関する脆弱性	JVN 掲載
11	Microsoft Windows と Internet Explorer に関する脆弱性	JVN 掲載
12	VERITAS Backup Exec の認証情報に関する脆弱性	JVN 掲載
13	EMC Legato NetWorker の認証機構に関する脆弱性	JVN 掲載
14	EMC Legato NetWorker の portmapper にリモートからの要求を実行する脆弱性	JVN 掲載
15	EMC Legato NetWorker の database service の認証機構に脆弱性	JVN 掲載
16	Apple 社の Mac 製品に複数の脆弱性	JVN 掲載
17	Microsoft DDS Library Shape Control(msdds.dll) COM オブジェクトにおける脆弱性	JVN 掲載
18	Computer Associates Message Queuing ソフトウェアに複数のバッファオーバーフローの脆弱性	JVN 掲載
19	pam_ldap に認証回避が可能な脆弱性	複数製品開発者に展開
20	simpleproxy における書式文字列に関する脆弱性	複数製品開発者に展開
21	Cisco IOS Firewall Authentication Proxy 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
22	Mozilla ベースのブラウザにおける、不正な IDN を含む URI 処理に関するバッファオーバーフロー脆弱性	JVN 掲載
23	X server に複数の整数バッファオーバーフローの脆弱性	複数製品開発者に展開
24	mod_ssl にクライアント認証の回避が可能な脆弱性	複数製品開発者に展開

表 2-5 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	MindAlign 製品に複数の脆弱性	複数製品開発者に展開
2	HP Ignite-UX に様々な脆弱性	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

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 379 件のうち、不受理のものを除いた 357 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。

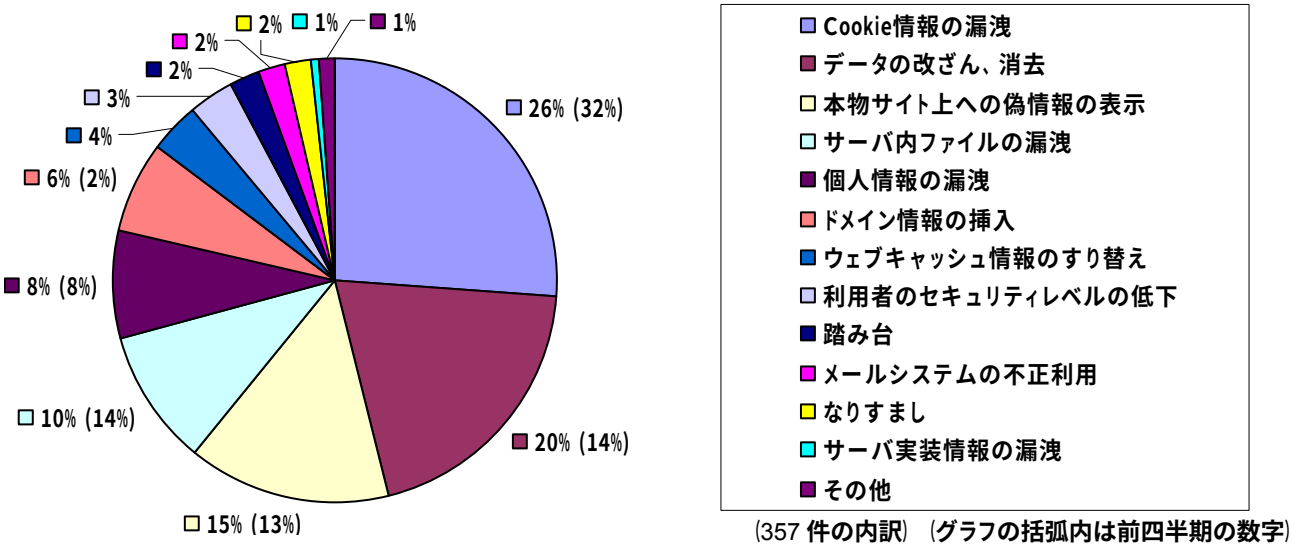


(357 件の内訳)　(グラフの括弧内は前四半期の数字)

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 9 月末まで) [6]

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」、「DNS 情報の設定不備」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 23 件のうち、12 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 11 件はエラーメッセージが表示されていただけで「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。



(357 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 9 月末まで)

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。

届出受付開始から 2005 年 9 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ウェ

[6] 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。

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図 3-3 に示します。全体の 86%の届出が、90 日以内に修正されています。脆弱性情報の届出を受理してから、ウェブサイト運営者に連絡するまでの日数は、平均 2 日以内です。

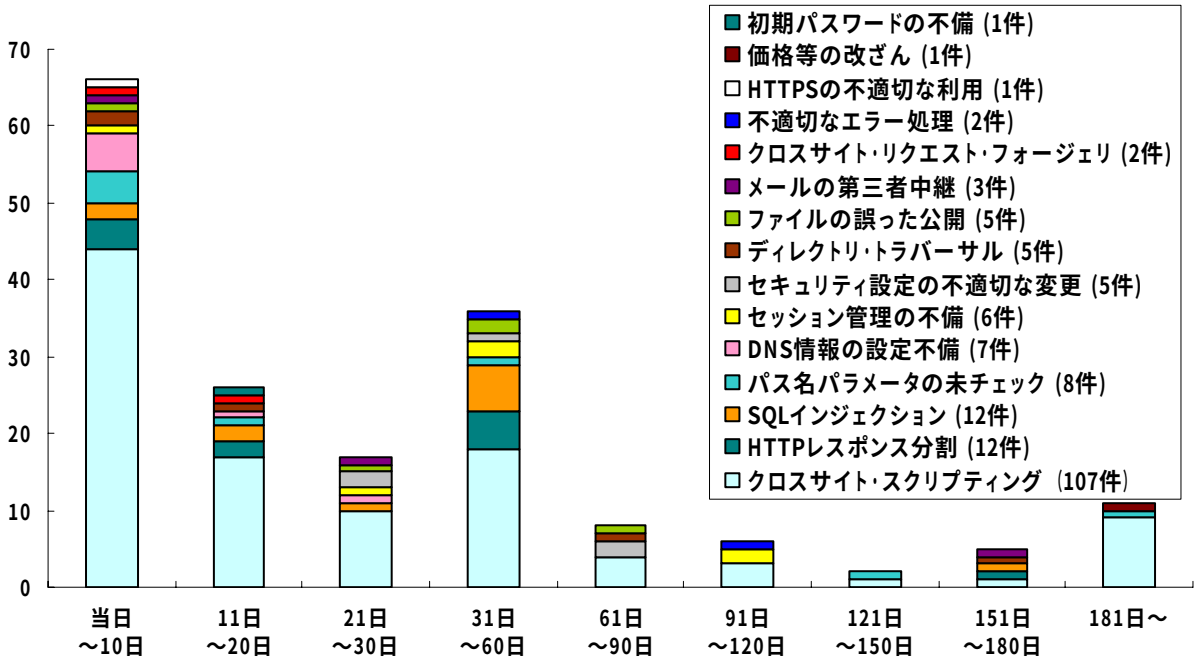


図 3-3 ウェブアプリケーションの脆弱性修正に要した日数

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**

  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。

- **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 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
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
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	セッション・ハイジャック 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 認証情報の漏洩
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
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
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
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
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 任意のスクリプトの実行 任意のファイルへのアクセス

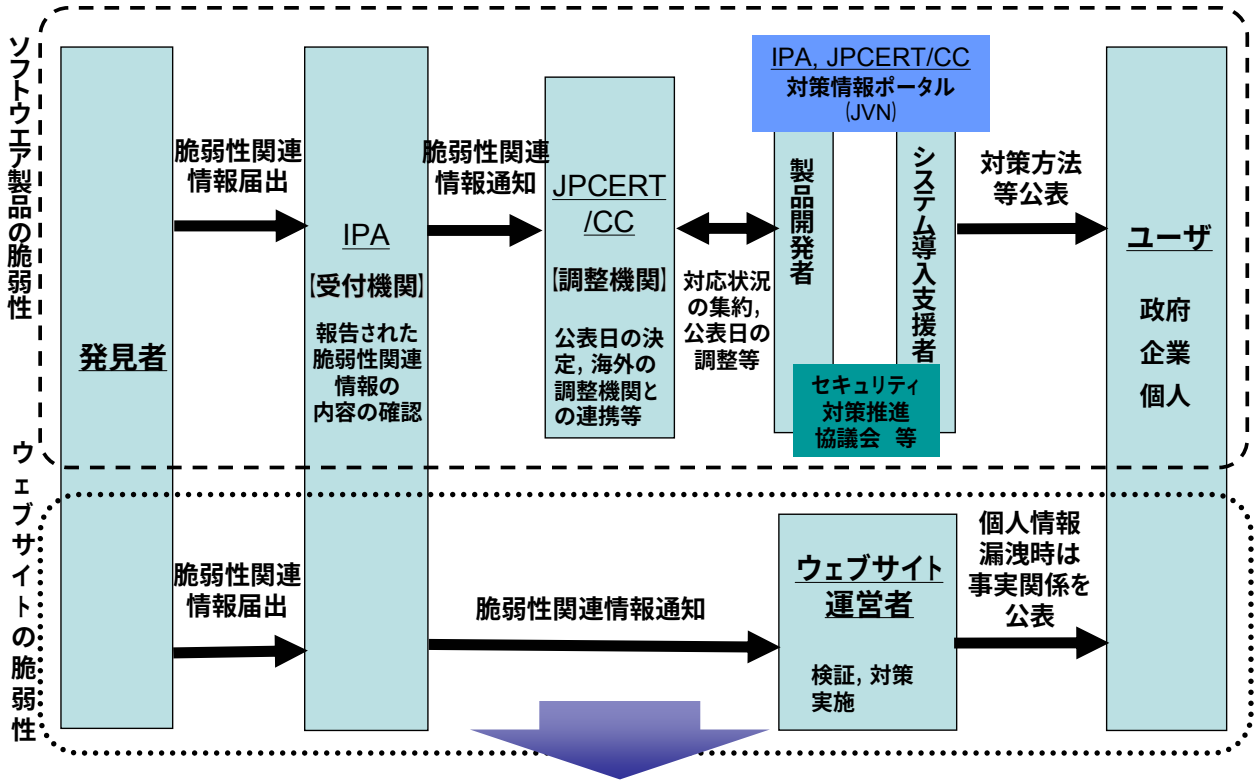
付表 2 ウェブアプリケーション脆弱性の分類

脆弱性の種類	深刻度	説明	届出において想定された脅威
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
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
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
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

脆弱性の種類	深刻度	説明	届出において想定された脅威
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
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

CGI : Common Gateway Interface
HTTP : HyperText Transfer Protocol
HTTPS : Hypertext Transfer Protocol Security
IDN : Internationalized Domain Name
IPv6 : Internet Protocol Version 6
ISP : Internet Service Provider
SQL : Structured Query Language
SSI : Server Side Include
SSL : Secure Socket Layer
TCP : Transmission Control Protocol
URI : Uniform Resource Identifier
URL : Uniform Resource Locator
VPN : Virtual Private 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：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）