プレスリリース
2009 年 3 月 17 日
独立行政法人情報処理推進機構

古いソフトウェア製品を利用しているウェブサイトへの注意喚起

ーウェブサイト運営者は脆弱性対策情報を収集し、修正プログラム（パッチ）の迅速な適用を!ー

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、「ソフトウェア製品に脆弱性が発見され、その開発者から修正プログラム（パッチ）が公表されているが、実際に運用しているウェブサイトがパッチを適用していないのではないか？」という旨の届出が増加している状況をふまえ、ウェブサイト運営者に対し脆弱性対策情報の収集とパッチの迅速な適用を呼びかけます。

ソフトウェアの脆弱性を狙った攻撃に対処するためには、攻撃が行われる前に、ソフトウェアに修正プログラム（パッチ）を適用する必要があります。近年、脆弱性の公表から、その脆弱性を狙った攻撃が発生するまでの間隔が短くなっており、ウェブサイト運営者は迅速な対応が求められます。

2008 年第 3 四半期頃から、多数のウェブサイトに対して「ソフトウェア開発者からパッチが公表されているが、ウェブサイト運営者がそのパッチを適用していないのではないか？」という旨の届出が増加していることから、IPA としては、ウェブサイト運営者に対して注意を喚起することとしました。

具体的には、2004 年 12 月に公表された「Namazu におけるクロスサイト・スクリプティングの脆弱性[1]」や、2005 年 10 月に公表された「OpenSSL におけるバージョン・ロールバックの脆弱性[2]」のパッチ未適用の可能性を指摘する届出が、2009 年 3 月 16 日までに 272 のウェブサイトに対してありました（図 1）。その運営主体別の内訳は、民間企業が 100 のウェブサイト、地方公共団体が 74、教育・学術機関が 37、団体（協会・社団法人）が 32、政府機関が 15 など広範囲にわたっています（図 2）。

IPA でまとめた「2008 年のコンピュータ不正アクセス届出状況[3]」では、実際に被害があった原因として「古いバージョンの使用・パッチ未適用」が第 2 位で 16 件あり 13%を占めています。実被害にあわないために、**ウェブサイト運営者は、自組織のウェブサイトが使用しているソフトウェアの脆弱性対策情報を収集し、未対策の場合はパッチの迅速な適用が必要です。**

脆弱性対策情報は、「脆弱性対策情報データベース JVN iPedia(http://jvndb.jvn.jp/)」や「脆弱性対策情報収集ツール MyJVN(http://jvndb.jvn.jp/apis/myjvn/)」により効率的に収集することが可能です。

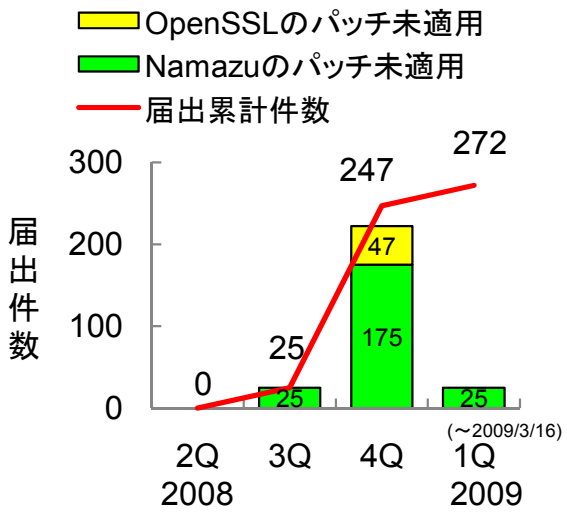

図1.パッチを未適用のウェブサイトに対する届出件数の期別推移

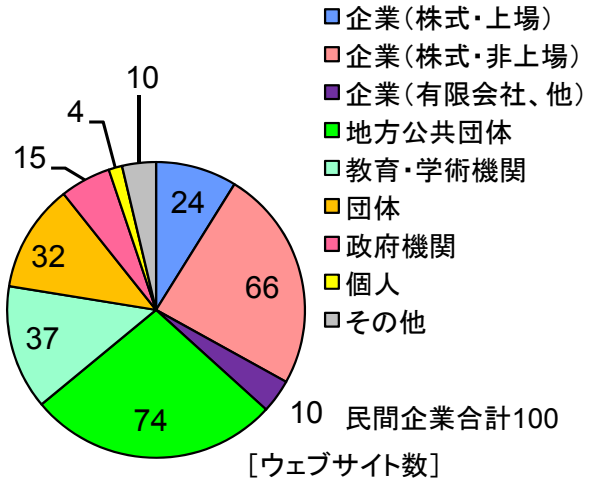

図2.パッチを未適用のウェブサイトに対する届出の運営主体の内訳

[1] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2004/JVNDB-2004-000554.html
[2] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2005/JVNDB-2005-000601.html
[3] 詳細は次の URL を参照下さい。http://www.ipa.go.jp/security/txt/2009/documents/2008all-cra.pdf

1. Namazu におけるクロスサイト・スクリプティングの脆弱性

2004 年 12 月 15 日に Namazu Project から公表された「日本語全文検索システム Namazu におけるクロスサイト・スクリプティングの脆弱性」に関するものです。

図 3 に示すように、ユーザのウェブブラウザ上で任意のスクリプトを実行されてしまう脆弱性があります。この脆弱性を悪用されると、偽ページの表示や、偽情報の流布による混乱、フィッシング詐欺による情報の漏えいなどの可能性があります。

また、Namazu には「pnamazu におけるクロスサイト・スクリプティングの脆弱性[4]」や「文字コードに起因したクロスサイト・スクリプティングの脆弱性[5]」なども公表されており、現時点では 2008 年 3 月 12 日に公開された Namazu 2.0.18 が対策版のため、この日付以前のものを使用している場合は、Namazu 2.0.18 以降の最新版への更新を推奨します。

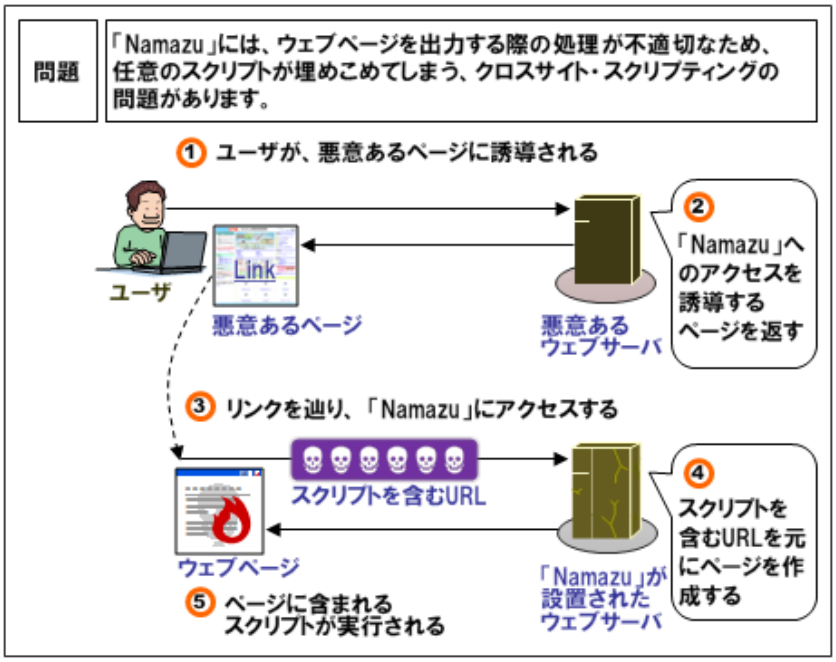

図 3.Namazu におけるクロスサイト・スクリプティングの脆弱性

2. OpenSSL におけるバージョン・ロールバックの脆弱性

2005 年 10 月 11 日に OpenSSL Project から公表された「OpenSSL におけるバージョン・ロールバックの脆弱性」に関するものです。図 4 に示すように、通信経路上で通信内容を細工されることにより、弱い暗号化通信方式を強制されてしまう脆弱性があります。この脆弱性を悪用されると、暗号化通信を希望しているクライアントとサーバ間のデータの盗聴や改ざんの可能性があります。

また、OpenSSL には「バッファオーバーフローの脆弱性[6]」や「サービス運用妨害 (DoS) の脆弱性[7]」なども公表されており、現時点では 2009 年 1 月 7 日に公開された OpenSSL 0.9.8j が対策版のため、この日付以前のものを使用している場合は、OpenSSL 0.9.8j 以降の最新版への更新を推奨します。

なお、OpenSSL を使用した OS やミドルウェアを開発している各社（サン・マイクロシステムズ社、レッドハット社、トレンドマイクロ社など）からも対策情報が公開されています。それぞれの情報を参照し、対策を実施する必要があります。

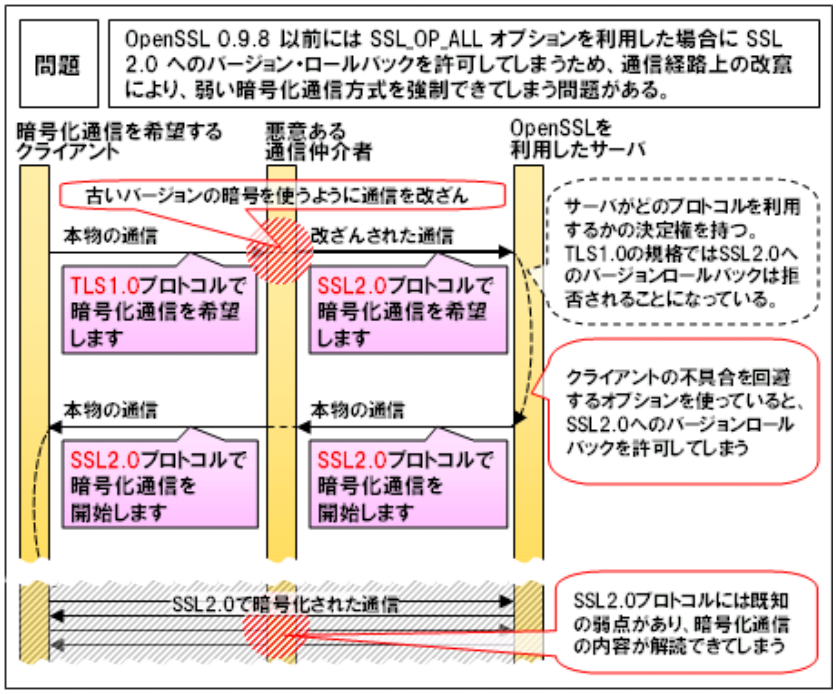

図 4.OpenSSL におけるバージョン・ロールバックの脆弱性

[4] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000851.html
[5] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-000018.html
[6] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000594.html
[7] 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001807.html

3.脆弱性対策情報の収集方法

3.1 脆弱性対策情報データベース JVN iPedia の活用

JVN iPedia(http://jvndb.jvn.jp/)は、日本国内で使用されているソフトウェア製品の脆弱性対策情報を収集するためのデータベースを目指し、(1) 国内のソフトウェア製品開発者が公開した脆弱性対策情報、(2) 脆弱性対策情報ポータルサイト JVN[8]で公表した脆弱性対策情報、(3) 米国立標準技術研究所 NIST[9]の脆弱性データベース「NVD[10]」が公開した脆弱性対策情報の中から情報を収集、翻訳し、2007 年 4 月 25 日から公開しており、2009 年 3 月現在、6,000 件を超える情報を格納しています。

JVN iPedia では、開発者ごとに公開されている脆弱性対策情報を一か所に集約することで、複数の開発者から情報を収集する手間を省き、効率的な情報収集を可能としています。また、さまざまな組織が公開する情報を横断的に知りたい場合や、特定のソフトウェアに存在する脆弱性について知りたい場合も、図 5 に示すような充実した検索機能によって効率的に情報を収集することができます。

さらに、検索結果一覧の中から、概要や影響を受けた時の深刻度、影響を受けるシステム、対策情報などの詳細な脆弱性対策情報が入手できます。

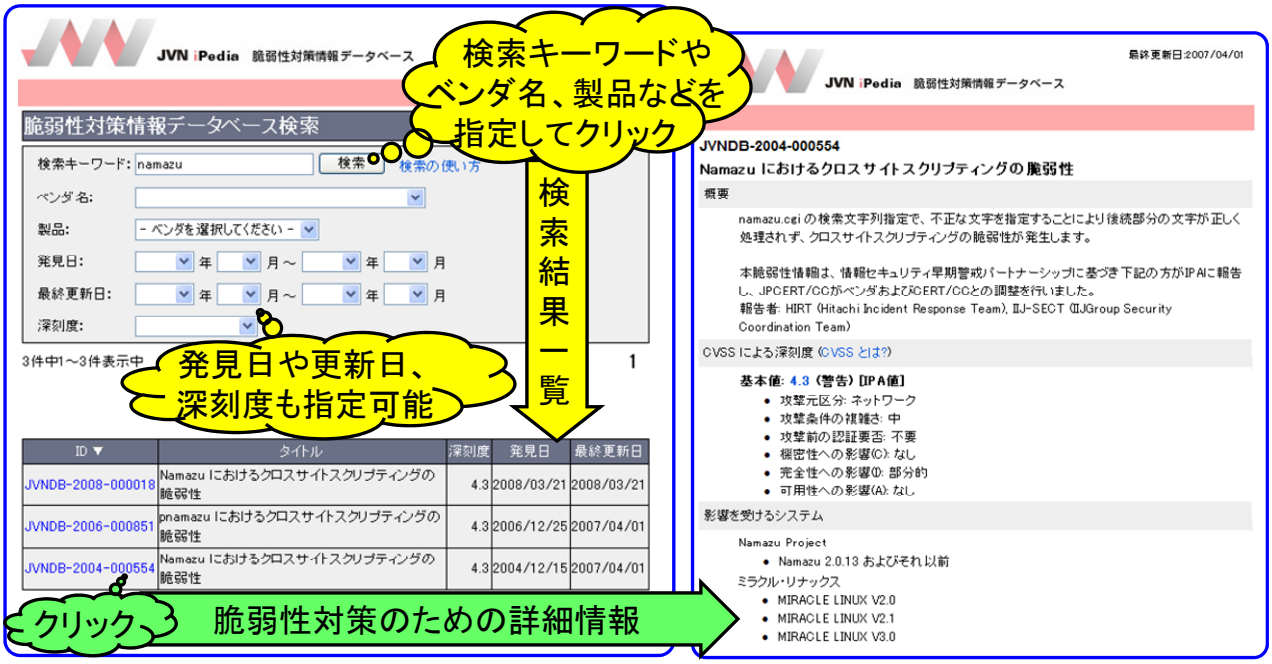

図 5.JVN iPedia の脆弱性対策情報の検索機能

3.2 脆弱性対策情報収集ツール MyJVN の活用

MyJVN(http://jvndb.jvn.jp/apis/myjvn/)は、JVN iPedia に登録された多数の情報の中から、利用者が、利用者自身に関係する情報のみを効率的に収集できるように、フィルタリング条件設定機能、自動再検索機能、脆弱性対策チェックリスト機能などを有し、2008 年 10 月 23 日から公開しています。

図 6 に示すように、利用者が収集したい製品開発者やソフトウェアなどのフィルタリング条件を一度設定しておけば、その後は MyJVN へアクセスするだけで、設定したソフトウェアの最新の情報だけが自動的に表示され、非常に効率的に情報を収集することができます。

さらに、脆弱性対策が具体的にどこまでできているか確認するための、脆弱性対策チェックリストを出力する機能も有しています。

---

[8] Japan Vulnerability Notes。脆弱性対策情報ポータルサイト。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。http://jvn.jp/

[9] National Institute of Standards and Technology。米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関。http://www.nist.gov/

[10] National Vulnerability Database。NIST が運営する脆弱性データベース。http://nvd.nist.gov/home.cfm

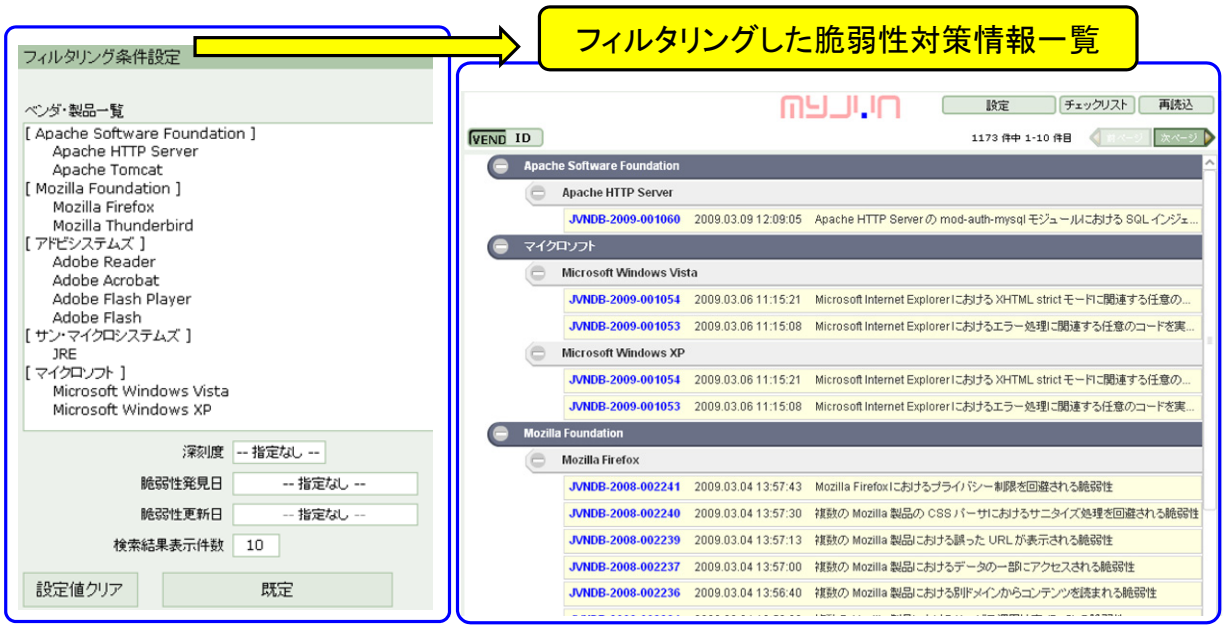

図 6.My JVN の脆弱性対策情報のフィルタリング機能

3.3 パッチ対策の緊急度の評価

IPA では脆弱性の深刻度を評価した CVSS[11]基本値を公表しています。JVN iPedia の CVSS 計算ツール（図 7）を用いると、各組織での対象製品の利用範囲や、攻撃を受けた場合の被害の大きさなどを考慮し、製品利用者自身が脆弱性への対応を判断ための CVSS 環境値を計算することが可能です。

この結果を基に、例えば CVSS 環境値が 7.0 以上は緊急にパッチ、4.0 以上は月次パッチ、それ以外は定期保守でパッチなど、パッチ対策の緊急度の見極めに活用できます。

図 7. JVN iPedia の CVSS 計算ツール

■ 本件に関するお問い合わせ先
IPA セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

[11] 共通脆弱性評価システム CVSS v2 概説。http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html