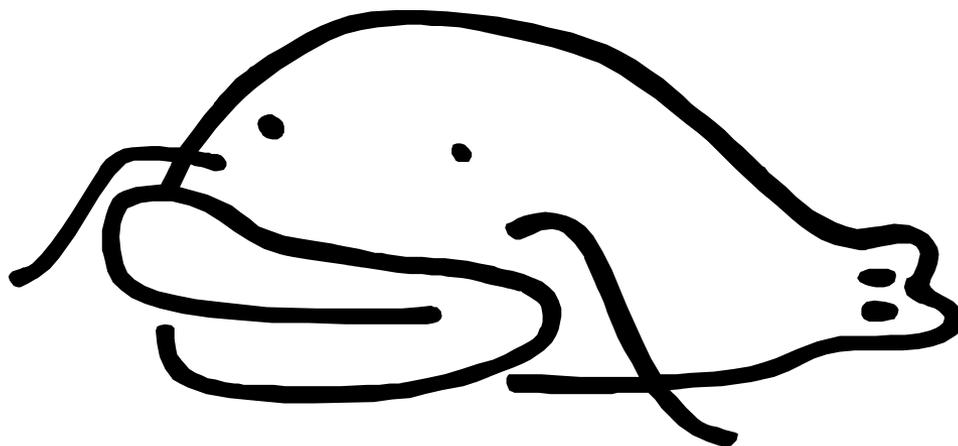


Namazu Project のインシデント対応
～ 中の人告白 ～



株式会社ドリーム・アーツ

竹迫 良範

<http://namazu.org/~takesako/>



近年のWebアプリ脆弱性情報の届出件数

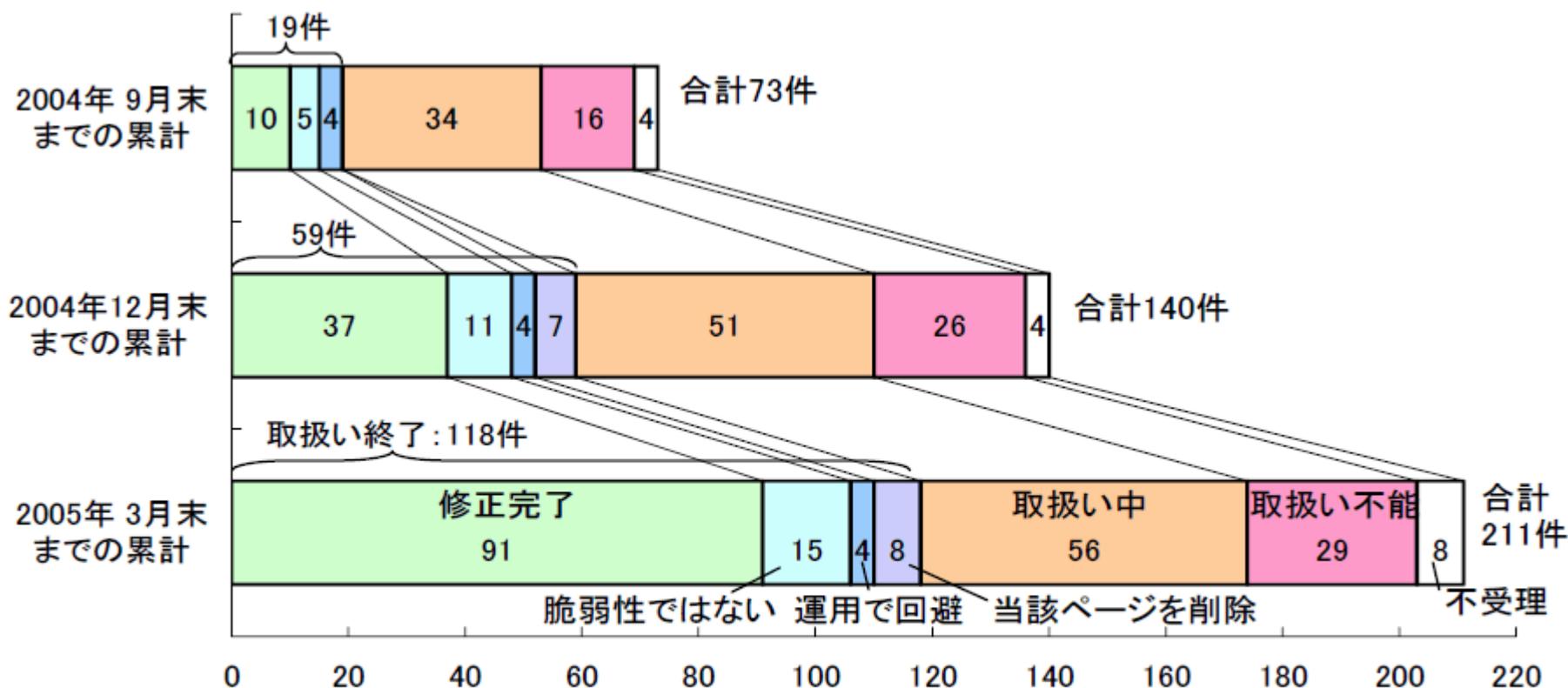


図 1-2 ウェブアプリケーション 脆弱性関連情報の届出の取扱い状況

※IPAソフトウェ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)より引用]



Webアプリ脆弱性の種類

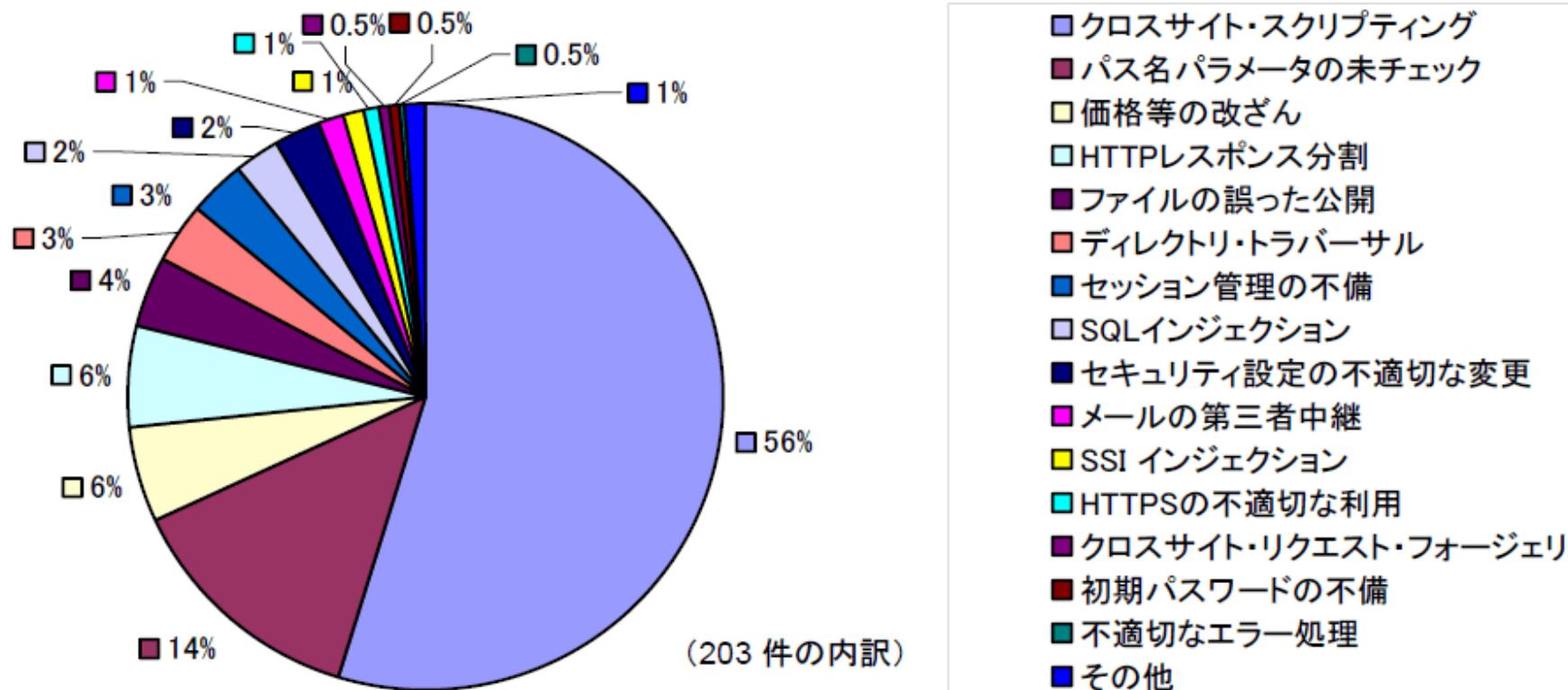


図 3-1 ウェブアプリケーションの脆弱性種類別内訳(届出受付開始から 2005 年 3 月末まで)

※IPAソフトウェ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)より引用]

はじまりは

突然



Date: Sun, 25 Nov 2001 19:03:46 +0900

Namazuz Project セキュリティご担当様:

私ども産業技術総合研究所のセキュリティ脆弱性研究におきまして、ウェブアプリケーションの安全性について調査しておりましたところ、Namazu v2.0.7 にクロスサイトスクリプティング (**cross-site scripting**) 脆弱性と呼ばれるセキュリティ上の問題点が存在していると推察されましたので、このことについて技術的な観点からお知らせいたします。

■ 問題点

=====

NamazuzをCGIとして利用する「namazu.cgi」には、HTMLを動的に生成する際にメタキャラクタの適切なエスケープ処理を怠っている個所が残存しています。

⋮



しかし事件はそのとき同時に起きていた・・・

From: "TAKAGI, Hiromitsu"

Date: Tue, 27 Nov 2001 16:46:31 +0900

私がお送りしたこのメールの宛先は、

> To: bug-namazu@xxxxxxxxxxx

でした。それが、namazu-devel-ja メーリングリストに流れて、
<http://www.namazu.org/ml/namazu-devel-ja/msg02114.html>
で公開状態になっていることを、今、知りました。

→ **なんと脆弱性の報告窓口が公開メーリングリストだった！**

Namazu is a full-text search engine. Namazu has an index maker, mknmz command, and a text searcher, namazu command. For searching a great amount of documents quickly, Namazu makes an index in advance. The concept of index is just similar to an index of book.

Namazu for Win32



翌々日に Namazu 2.0.8 をリリース

The screenshot shows a Microsoft Internet Explorer browser window with the address bar containing the URL: <http://slashdot.jp/article.pl?sid=01/11/27/1024251&mode=nested>. The page content includes the OpenLDAP logo and "Developers wanted" text. The main article title is "Namazu 2.0.8 リリース". The article text reads: "knok による 2001年11月27日 19時19分の投稿, セキュリティには気を付けよう 部門より. Namazu Project より 2.0.8 をリリースします. 今回の変更点は cross-site scripting 脆弱性の修正のみです. サーバ側に対しなんらかの影響があるような、いわゆる remote exploit ではありませんが、クライアント側になんらかの影響を与える可能性があります. 特に cookie を併用しているような場合では注意が必要です. 今回のリリースに合わせて、[Namazuのセキュリティに関する考察](#)も更新しました. 合わせてみていただけると幸いです." The article is accompanied by a small Namazu logo. The page also features a sidebar with navigation links like "ログイン", "アカウント取得", "ストーリー", and "Slashdot".



早速セキュリティ関連の報告窓口を新設

「こっそり」という表現をしていながら一般に公開されるアドレスにリンクを貼っていたのはこちらの落度であり、高木先生になんら非はありません。

新たに security@xxxxxxxxxx という非公開なアドレスを用意し、このページには今後はそちらへリンクするようしておきます。

幸い既にパッチもできていますし、今回の件が重大と感じた方は今からでもパッチを適用して対策を行なうことをお勧めします。

⋮

しかかし!

これだけで話は
終わらなかつた



開発者自身が別の脆弱性を発見… |_|_|○

From: `knok@xxxxxxxxxxxxxx` (NOKUBI Takatsugu)

Date: Thu, 29 Nov 2001 19:19:45 JST

新たに別の問題が発生しました... すでに CVS の方へでは fix しておきましたので、明日にも 2.0.9 をリリースしようと思います。

新しい test script を作成して、今回のような vulnerability を検証するようにしたので、今後はそう頻繁に問題が出ることはないと思います(と信じたい)。

テスト可能な方は、make check してみてくださいませんか。

Namazuz is a full-text search engine. Namazu has an index maker, mknmz command, and a text searcher, namazu command. For searching a great amount of documents quickly, Namazu makes an index in advance. The concept of index is just similar to an index of book.

Namazuz for Win32



翌日 Namazu 2.0.9 をリリース

The screenshot shows a Microsoft Internet Explorer window with the address bar containing the URL: <http://slashdot.jp/article.pl?sid=01/11/30/0817222&mode=nested>. The page content includes the Slashdot logo with the tagline "News for Nerds. Stuff that matters." and a navigation menu with links for "ログイン", "アカウント取得", "ストーリー", "古いストーリー", "過去の投票", "殿堂入り", "トピック", "日記ページ", "Slashdot", "About us", "プライバシー", "編集者紹介", "FAQ", "コード", and "オリバー日記". The main article is titled "Namazu 2.0.9 リリース" and is dated "2001年11月30日 17時13分". The text of the article reads: "knok による 2001年11月30日 17時13分の投稿, チェックが甘い 部門より. Namazu 2.0.9 をリリースしました. 今回もクロスサイトスクリプティング問題を修正するためのリリースです. 同じ轍は踏むまいと test case を書いたら, 他のもところにも同じバグをみつけてしまいました...不手際が多くて申し分けなのですが, 再度入れ替えをお願いします. しかし, test case を整備したことで, 今後同じバグを発生させる可能性はかかなり減らせたと思います." A small Namazu mascot icon is visible next to the article text. On the right side of the browser window, there is a login form for "Slashdot Japan" with fields for "ニックネーム:" and "パスワード:", a "ログイン" button, and links for "[新しいアカウントを作る]" and "[パスワードを忘れた]". Below the login form is a "関連リンク" section with a link to "Namazu".

(/Д`) ...

それから

長く平和な日々が
訪れるはずだった



3週間後にまた別の脆弱性が発覚 |_|_|○

From: knok@xxxxxxxxxxxxxx (NOKUBI Takatsugu)

Date: Mon, 17 Dec 2001 15:28:05 JST

namazu-2.0.10rc1 の用意をしました。
<<ftp://ftp.namazu.org/namazu/test/namazu-2.0.10rc1.tar.gz>>

とある方より指摘のあった、さらなる cross-site scripting の修正と、コードレベルでの検証による buffer overflow の可能性の除去が今回の変更内容になります。

検証した限り、外部からの入力での buffer overflow になることはありませんが、いくつか local に buffer overflow を起こすことのできる部分がありましたので、その点を修正しました。

[namazu/namazu.cgi](#) は setuid して利用するような性質のものではないので、
大きな危険はないと思います... 一応。

Namazuz is a full-text search engine. Namazu has an index maker, mknmz command, and a text searcher, namazu command. For searching a great amount of documents quickly, Namazu makes an index in advance. The concept of index is just similar to an index of book.

Namazuz for Win32



そして Namazu 2.0.10 をリリース

スラッシュドット ジャパン | Namazu 2.0.10 リリース - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

検索 お気に入り 履歴

アドレス(D) http://slashdot.jp/article.pl?sid=01/12/27/0546223&topic=87&mode=thread

リンク

OSDN Japan: イベント - JLCメマガ - JLC日記 - RSS - 広告掲載

検索: [] Go

コンテンツ事業者様へ
ISP事業者様へ

Slashdot
News for Nerds. Stuff that matters.

ログイン
アカウント取得

ストーリー
古いストーリー
過去の投票
殿堂入り
トピック
日記ページ

Slashdot
About us
プライバシー
編集者紹介
FAQ
コード
オリバー日記

Namazuz 2.0.10 リリース

knok による 2001年12月27日 14時30分 の投稿,
何度もすいません 部門より.

Namazuz 2.0.10 をリリースしました。

さらに残っていた cross-site scripting を修正しました。この機会にコードを再度検証しなおし、今度こそ修正しぎったと思います...

同時に buffer overflow の可能性についても検証しました。過去のバージョンでも、少なくとも外部からの入力で buffer overflow を起こすことはありませんが、今回は可能性のある部分をできる限り修正しましたので、より安全になったと思います。

スラッシュドット ジャパン
ログイン

ニックネーム:
パスワード:

ログイン

[新しいアカウントを作る]
[パスワードを忘れた]

関連リンク

- Namazuzのほかの記事
- knokのほかの記事

インターネット

(。´Д<)



さらに特定の環境での脆弱性が報告される

From: HANAI Akira <hanai-a@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Date: Tue, 26 Mar 2002 13:24:58 +0900

花井と申します。

社内のイントラネットにてnamazuを使用させていただいております。

クロスサイトスクリプティングに対する脆弱性ではないかと思われる現象がありました。

cgiの呼び出しにて、存在しないインデックスを

http://~/cgi-bin/namazu.cgi.exe?idxname=hoge

と指定すると、下記のようなエラーが返ってきます。

namazu: D:\ynamazuyv\ynamazuyindex\hoge\NMZ.head: No such file or directory

namazu: D:\ynamazuyv\ynamazuyindex\hoge\NMZ.body: No such file or directory

namazu: D:\ynamazuyv\ynamazuyindex\hoge\NMZ.foot: No such file or directory

この時、http://~/cgi-bin/namazu.cgi.exe?idxname=hoge の様に、インデックス名にタグを含めると、エラー内容の表示でタグが有効なまま表示されます。(上記エラーでいえば~を付けると「hoge」が太字で表示される。)

<script>等のタグも有効になるようですので、クロスサイトスクリプティングに繋がる問題ではないかと思い報告致します。

【検証結果】

* IIS4.0 / WindowsNT4.0

* IIS5.0 / Windows 2000

→ 標準エラー出力が、

ブラウザに表示されてしまう。

●AN HTTP 1.39f / WindowsNT4.0

→ 標準エラー出力は、

ブラウザに出力されない。

IIS固有の問題？



標準エラー出力による問題

- 2.0.10 以前までの namazu.cgi は警告などを標準エラー出力に出力していましたが、一部の web server の実装は標準エラー出力と標準出力を同一に扱うものがあり、その結果クロスサイトスクリプティング問題を引き起こすことがありました。具体的には Microsoft の Internet Information Server 4.0, 5.0 が該当します。
- この問題を解決するために、2.0.11以降では NMZ.warnlog というファイルに警告を出力するよう変更して対処しました。
- CGI の仕様には、標準エラー出力の扱いについては言及されていません。おそらくは web server 側の問題だとは思われますが、こういった問題のある実装がある以上、CGI 作成者はこの点に注意する必要があると思われま

Namazu is a full-text search engine. Namazu has an index maker, mknmz command, and a text searcher, namazu command.
For searching a great amount of documents quickly, Namazu makes an index in advance.
The concept of index is just similar to an index of book.

Namazu for Win32



またまた Namazu 2.0.11 / 2.0.12 をリリース

セキュリティホール memo - 2002.09 - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

← 戻る → 進む × 閉じる 検索 お気に入り 履歴

アドレス(D) http://www.stryukoku.ac.jp/~kjm/security/memo/2002/09.html#20020903_namazu 移動

リンク

■ [Namazu 2.0.12 released](#)
(annouce-ja@namazu.org ML, Tue, 03 Sep 2002 15:49:19 +0900)

[Namazu](#) 最新版 2.0.12 が登場しています。[標準エラー出力による問題](#) (クロスサイトスクリプティング問題につながってしまう) などが排除されています。Namazu 利用者にはなにはともあれ upgrade しておきましょう。IIS 4.0/5.0 上で Namazu を利用している場合は特に。

参照: [クロスサイトスクリプティング脆弱性\(ver2.0.10\)](#) (namazu-devel-ja ML)

インターネット

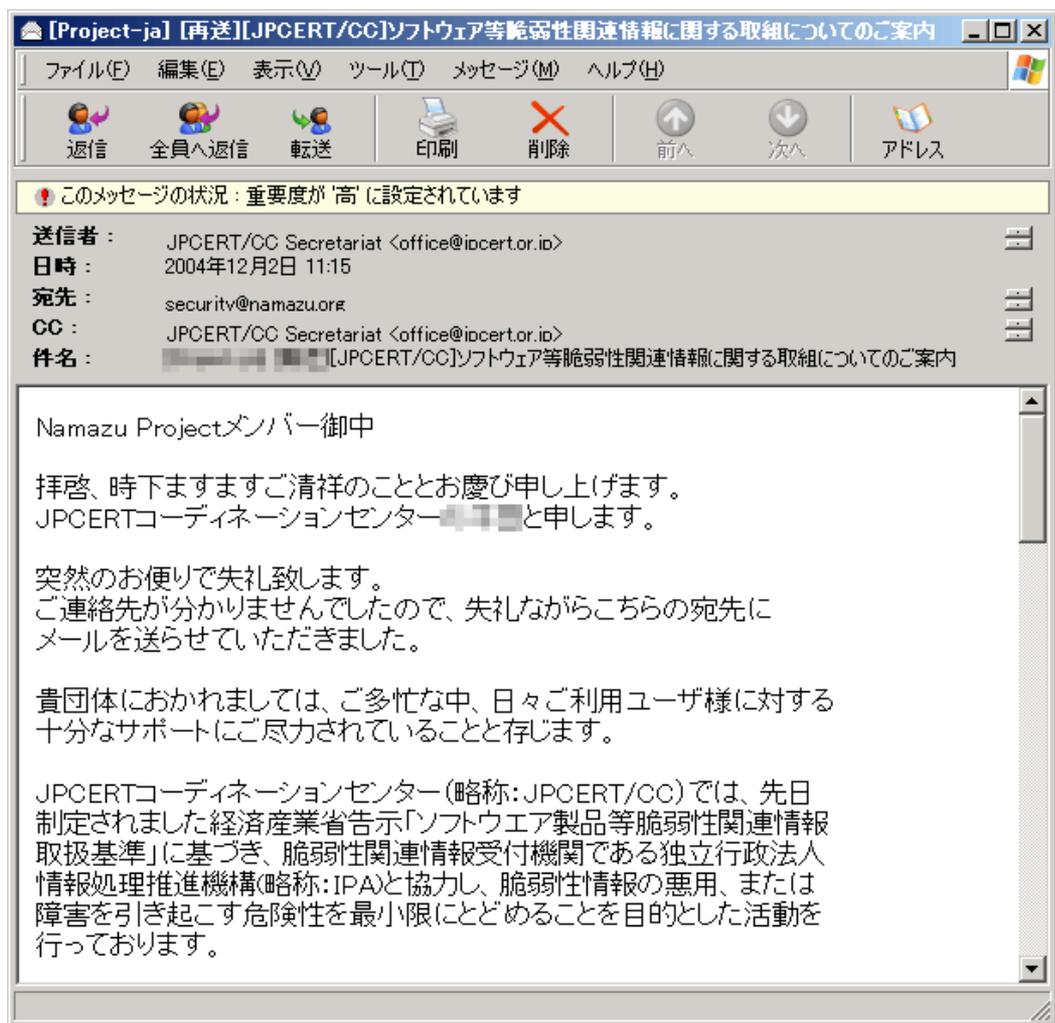
(。´Д<)

そして・・・

平穏な一年が過ぎ
たある日の出来事



JPCERT/CCから突然メールが届いた



→ 電話で問い合わせてみることに

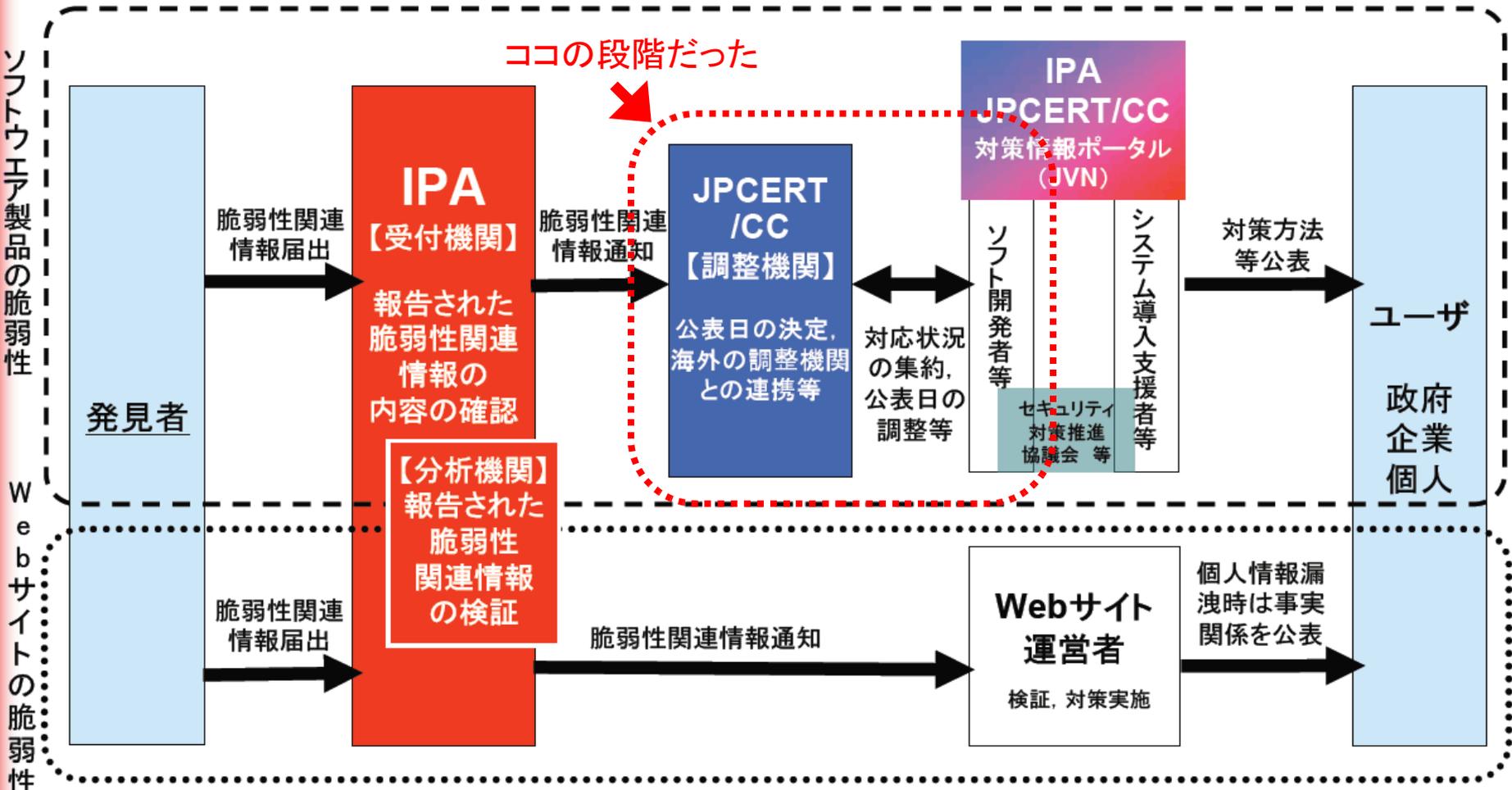


Namazu 2.0.13 に存在した脆弱性

- タブ(%09) から始まる検索文字列による問題
 - Namazu 2.0.13 以前までの namazu.cgi はタブ(%09)から始まる検索文字列を指定すると、検索文字列がサニタイズされなくなり、クロスサイトスクリプティング脆弱性が発生します。
- バージョンアップによる対応
 - 報告を受け、Namazu 2.0.14 以降では先頭のタブを削除することで、この問題に対処しました。(adhoc対応)
- ワークアラウンドの提示
 - Shellスクリプト、Perlスクリプトによる wapper
 - バージョンアップがすぐにできない人のため



脆弱性情報ハンドリングの概要



Namazu is a full-text search engine. Namazu has an index maker, mknmz command, and a text searcher, namazu command. For searching a great amount of documents quickly, Namazu makes an index in advance. The concept of index is just similar to an index of book.



Namazu 2.0.14 のリリース

Vendor Status Notes — JP

JVN#904429FE

Namazu におけるクロスサイトスクリプティングの脆弱性

概要

namazu.cgi の検索文字列指定で、不正な文字を指定することにより後続部分の文字が正しく処理されず、クロスサイトスクリプティングの脆弱性が発生します。

影響を受けるシステム

- Namazu 2.0.13 およびそれ以前

想定される影響

Webサイト上で namazu.cgi を使用して検索処理を実現している全てのサイトでクロスサイトスクリプティングの脆弱性が存在し、ページ内容の改竄、Cookie 情報の奪取等が可能になります。

ベンダ情報

製品開発者リスト登録ベンダ

| ベンダ | ステータス | 更新日 |
|--------------------------------|--------|------------|
| Namazu Project | 該当製品あり | 2004/12/15 |

謝辞

本脆弱性情報は、情報セキュリティ早期警戒パートナーシップに基づき下記の方が IPA に報告し、JPCERT/CC がベンダとの調整を行いました。

報告者: HIRT (Hitachi Incident Response Team), IJ-SECT (IJGroup Security Coordination Team)

Vendor Status Notes — JP

2005 | 2004

2005

- JVN#466742E: Wiki クローンにおけるクロスサイトスクリプティングの脆弱性
- JVN#A46697B1: 「ウイルスセキュリティ」におけるメモリークの脆弱性
- JVN#8ED8A96: 「ウイルスセキュリティ」におけるヒープオーバーフローの脆弱性
- JVN#74012178: Movable Type におけるセッション管理の脆弱性
- JVN#AF02FB4B: nProtect : Netizen における脆弱性
- JVN#A7DA8818: WebUD における任意のプログラムが実行される脆弱性
- JVN#97757029: w3ml におけるクロスサイトスクリプティングの脆弱性
- JVN#55023557: パフアロー製ルータにおける設定画面のリモートアクセスとパスワード漏洩の脆弱性
- JVN#9ADCBB12: 携帯電話端末における特定 QR コードを使用したサイト接続時の問題
- JVN#55F159B6: ppBlog におけるクロスサイトスクリプティングの脆弱性
- JVN#23D7E89F: 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
- JVN#C45D8EAD: Norton AntiVirus で不正なファイルのスキャン時に OS 異常終了
- JVN#1F649902: 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
- JVN#DD18AD07: Tomcat におけるサービス拒否の脆弱性
- JVN#8BAAB4E: msearch におけるディレクトリトラバーサル脆弱性
- JVN#8F8B1C85: 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
- JVN#1BF8D7AA: LDAP サーバの更新機能におけるバッファオーバーフロー脆弱性

2004

- JVN#B4BE09A4: Shinken Pro 3.0 S/MIME 機能で署名検証時に証明書の実証性が確認されない
- JVN#904429FE: Namazu におけるクロスサイトスクリプティングの脆弱性
- JVN#B410A83F: Shinken Pro 3.0 S/MIME 機能で署名検証時に From: フィールドが確認されない
- JVN#7C9208F1: Beckyl Internet Mail における S/MIME の署名検証に脆弱性
- JVN#E59B594E: 鶴亀メールにおける S/MIME の署名検証に脆弱性
- JVN#61857DA9: DNSキャッシュサーバの TCP SYN_SENT 状態によるリソース消費
- JVN#E7DDE712: 東芝製HDD&DVDビデオレコーダーへ認証なしでアクセス可能
- JVN#67B82FA3: SSL-VPN製品におけるCookieの脆弱性
- JVN#F88C2C13: desknet's における脆弱性 (JVN#89DE2014 の情報を追加)
- JVN#FF73142E: ウィルスバスターコーポレートエディションに脆弱性

→ 脆弱性情報と同時に2.0.14を公開



参加ベンダーのリスト

アライドテレシス株式会社
株式会社インターネットイニシアティブ
日本エフ・セキュア株式会社
株式会社オムニサイソフトウェア
株式会社オレンジソフト
きてーや. ねっと
クオリティ株式会社
コンピュータ・アソシエイツ株式会社
有限会社サイトー企画
サイボウズ株式会社
三洋電機株式会社
JNS株式会社
シスコシステムズ株式会社
株式会社シマンテック
シャープ株式会社
株式会社ジャストシステム
ソースネクスト株式会社
ターボリナックス株式会社
有限会社 デージーネット
テクマトリックス株式会社
株式会社デンソーウェーブ

株式会社 東芝
東芝ソリューション株式会社
トレンドマイクロ株式会社

NamazuzProject

日本電気株式会社
日本ユニシス株式会社
株式会社ビー・ユー・ジー

HikiDevelopmentTeam

株式会社日立製作所
株式会社ヒューコム

PukiWikiDevelopersTeam

富士通株式会社

FreeStyleWikiプロジェクト

古河電気工業株式会社
ボーダフォン株式会社
株式会社ホライズン・デジタル・エンタープライズ
三菱電機株式会社
ミラクル・リナックス株式会社
毛流麦花
ヤマハ株式会社
横河電機株式会社
株式会社リコー
有限会社リムアーツ

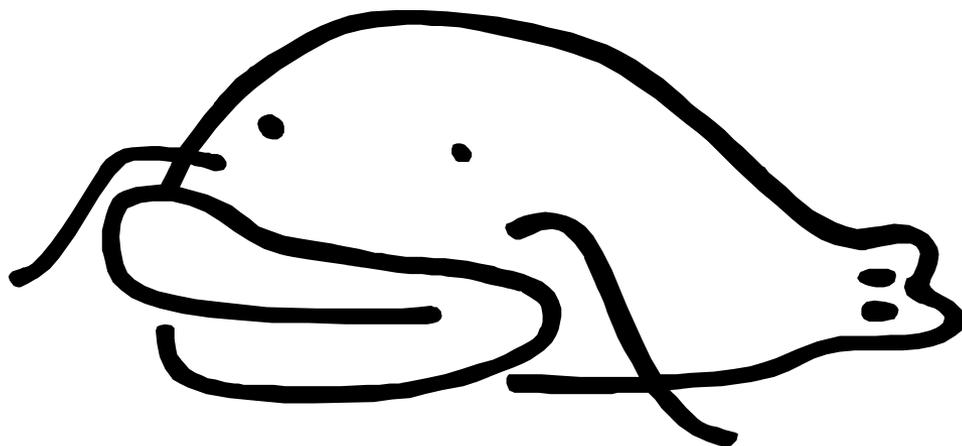
※2005年6月3日現在
<http://jvn.jp/nav/>



これまでの教訓(まとめ)

- セキュリティ関連専用の報告窓口を設置する
 - オープンソースと言えどもセキュリティ関連のやりとりはオープンにせず、非公開とする
security@xxxxxxxxxxx
- 脆弱性を修正したら、修正を確認するテストスクリプトを書く
 - Test suites (test program + test data) いろんな環境でテスト
- 古いコードを放置しない(場合によってはリファクタリング)
 - 他の脆弱性がないかどうかもう一度検証する
- リリースを急ぎすぎない(対応をあせらない)
 - もっとじっくりとコードを検証していれば余計な問題は発覚していなかったかも

いつもNamazuのバグ・脆弱性発見時は
紳士的な対応をありがとうございます



これからもNamazuをよろしくお願いします