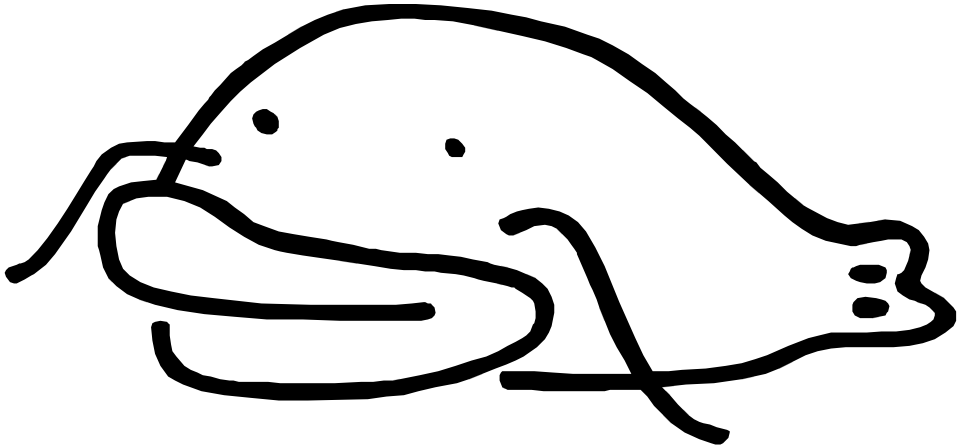
Linux CONFERENCE 2005

Lightning Talk

Namazu Project のインシデント対応
～　中の人の告白　～



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

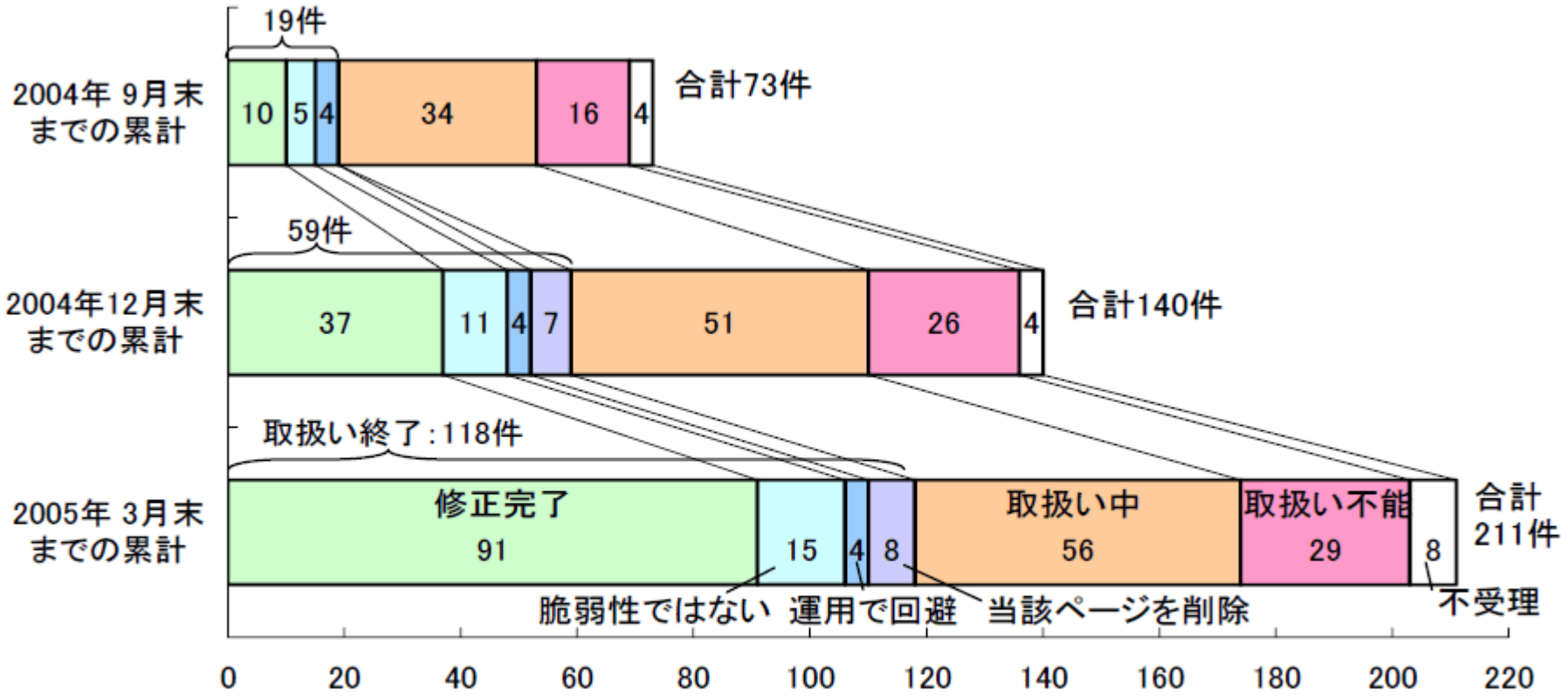


図 1-2 ウェブアプリケーション 脆弱性関連情報の届出の取扱い状況

※IPAソフトウエ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

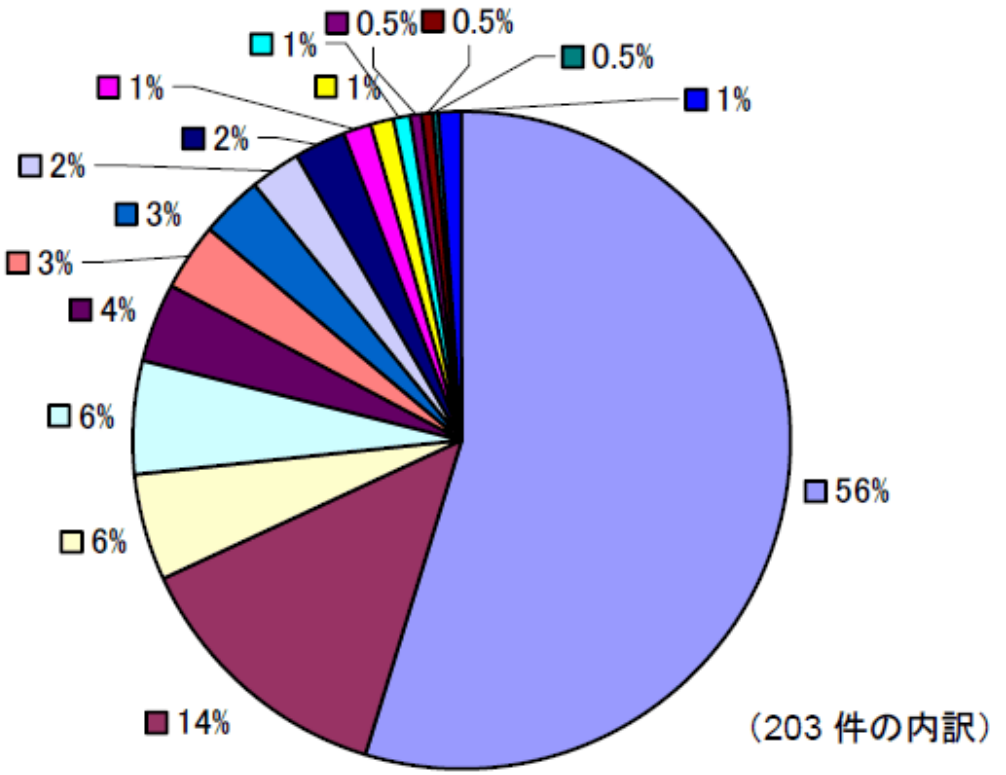


図 3-1 ウェブアプリケーションの脆弱性種類別内訳(届出受付開始から 2005 年 3 月末まで)

※IPAソフトウエ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

Namazu 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
=========
Namazu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@xxxxxxxxxx

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！

翌々日に Namazu 2.0.8 をリリース

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にしておきます。

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薦めします。

：
：

しかし!

これだけで話は終わらなかった

開発者自身が別の脆弱性を発見… _|￣|○

From: knok@xxxxxxxxxxxxx (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 してみていただけませんでしょうか。

翌日 Namazu 2.0.9 をリリース

(ﾉ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@xxxxxxxxxxxx (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 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。

そして Namazu 2.0.10 をリリース

(。´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@xxxxxxxxxxxxxxxxxxxxxx>
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:ynamazuyvarynamazuyindex/hoge/NMZ.head: No such file or directory
namazu: D:ynamazuyvarynamazuyindex/hoge/NMZ.body: No such file or directory
namazu: D:ynamazuyvarynamazuyindex/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ませると、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。

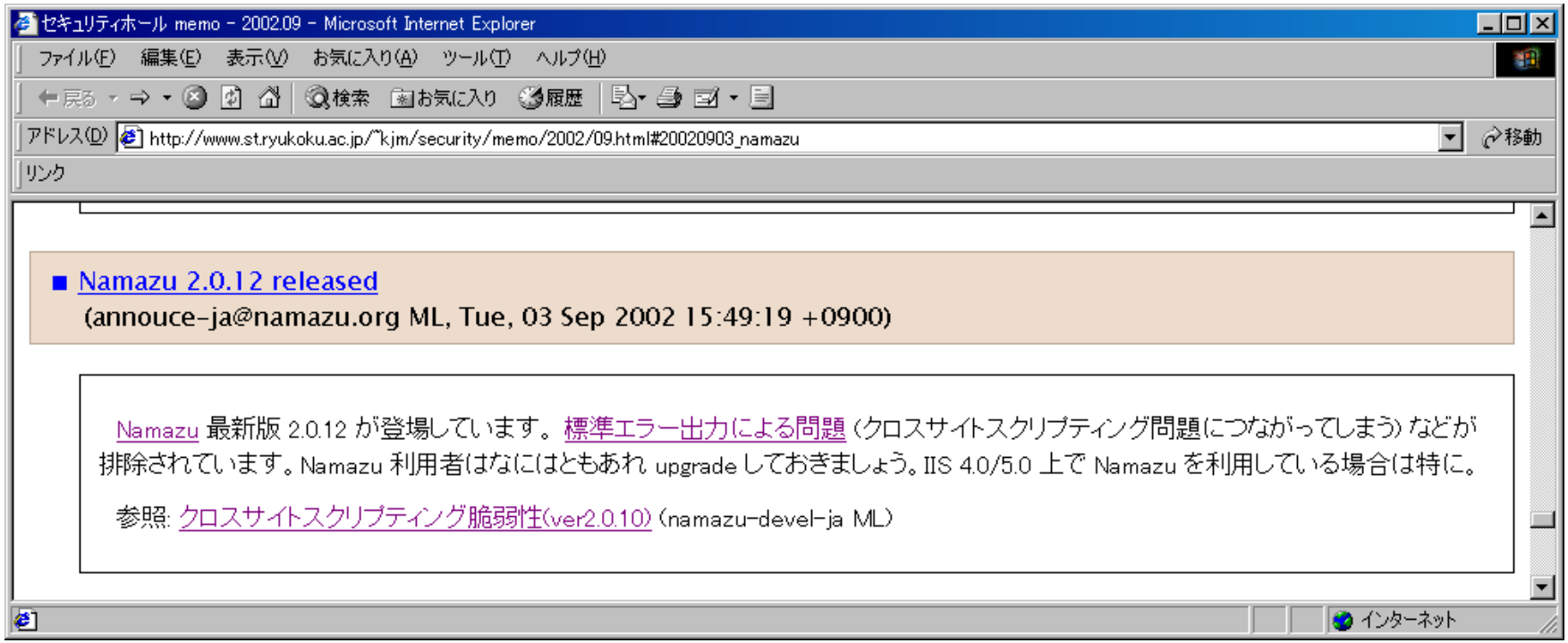
•AN HTTP 1.39f / WindowsNT4.0
→ 標準エラー出力は、
ブラウザに出力されない。

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す

またまた Namazu 2.0.11 / 2.0.12 をリリース

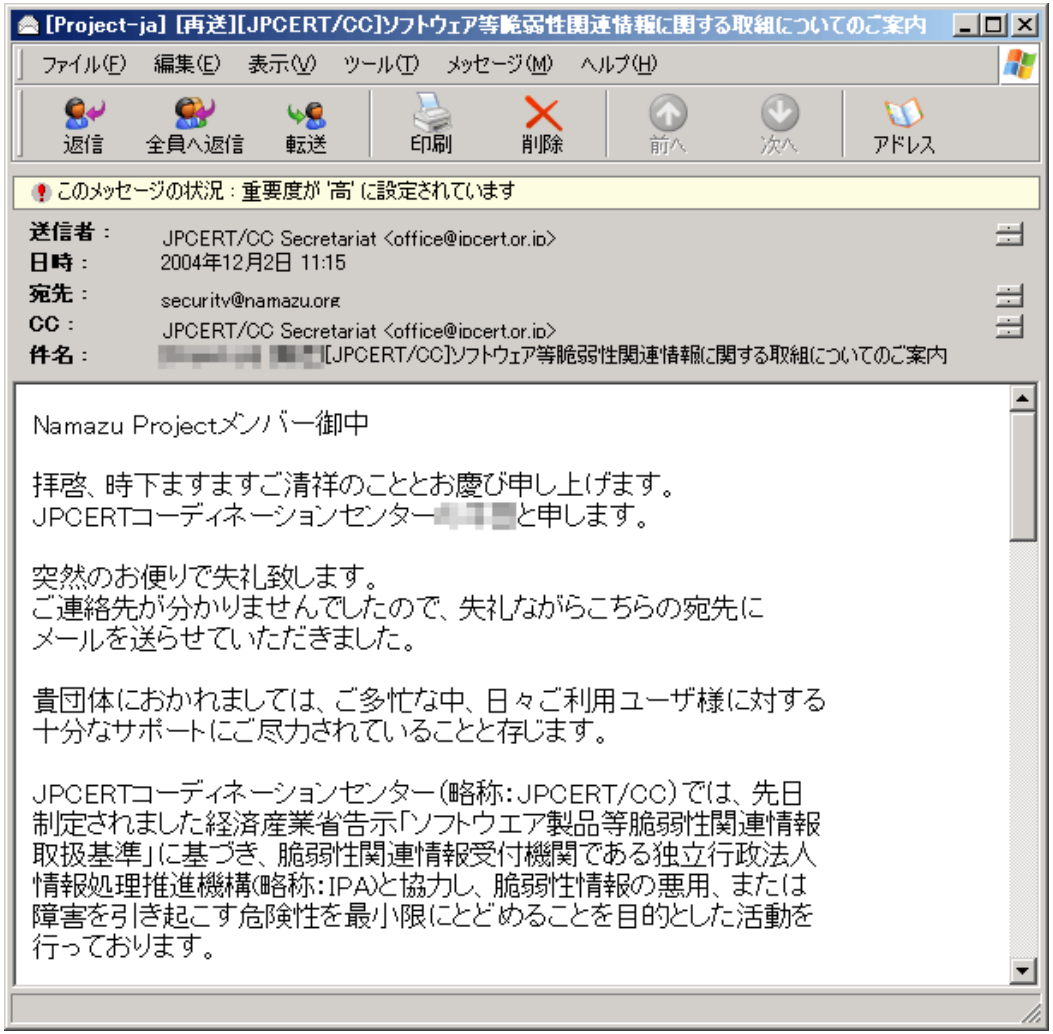


(。´Д⊂)

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



[Project-ja] [再送][JPCERT/CC]ソフトウェア等脆弱性関連情報に関する取組についてのご案内

ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)

返信 全員へ返信 転送 印刷 削除 前へ 次へ アドレス

このメッセージの状況：重要度が '高' に設定されています

送信者： JPCERT/CC Secretariat <office@jpcert.or.jp>
日時： 2004年12月2日 11:15
宛先： security@namazu.org
CC： JPCERT/CC Secretariat <office@jpcert.or.jp>
件名： [JPCERT/CC]ソフトウェア等脆弱性関連情報に関する取組についてのご案内

Namazu Projectメンバー御中

拝啓、時下ますますご清祥のこととお慶び申し上げます。
JPCERTコーディネーションセンター[redacted]と申します。

突然のお便りで失礼致します。
ご連絡先が分かりませんでしたので、失礼ながらこちらの宛先に
メールを送らせていただきました。

貴団体におかれましては、ご多忙な中、日々ご利用ユーザ様に対する
十分なサポートにご尽力されていることと存じます。

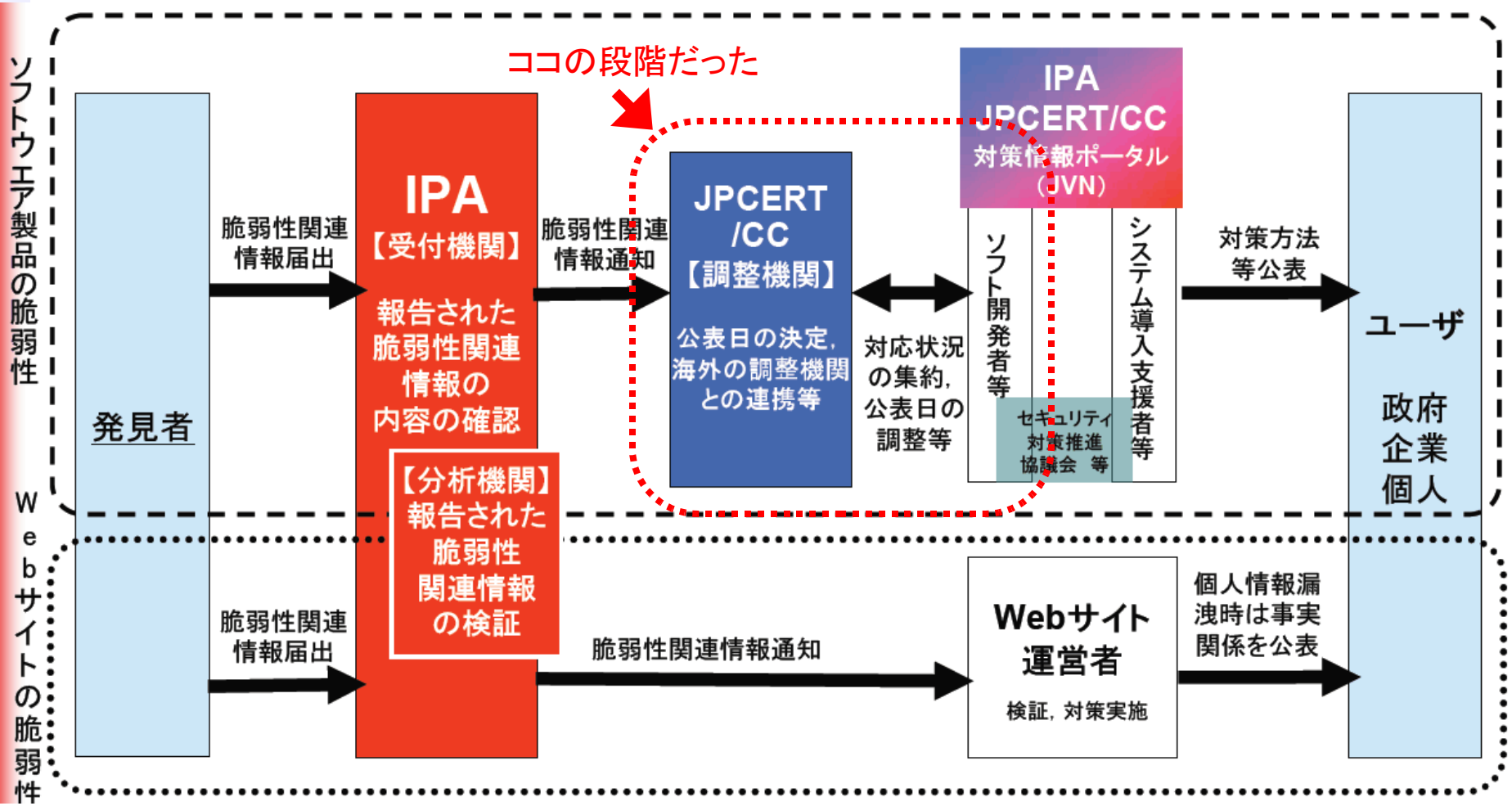
JPCERTコーディネーションセンター(略称:JPCERT/CC)では、先日
制定されました経済産業省告示「ソフトウエア製品等脆弱性関連情報
取扱基準」に基づき、脆弱性関連情報受付機関である独立行政法人
情報処理推進機構(略称:IPA)と協力し、脆弱性情報の悪用、または
障害を引き起こす危険性を最小限にとどめることを目的とした活動を
行っております。

→ 電話で問い合わせてみることに

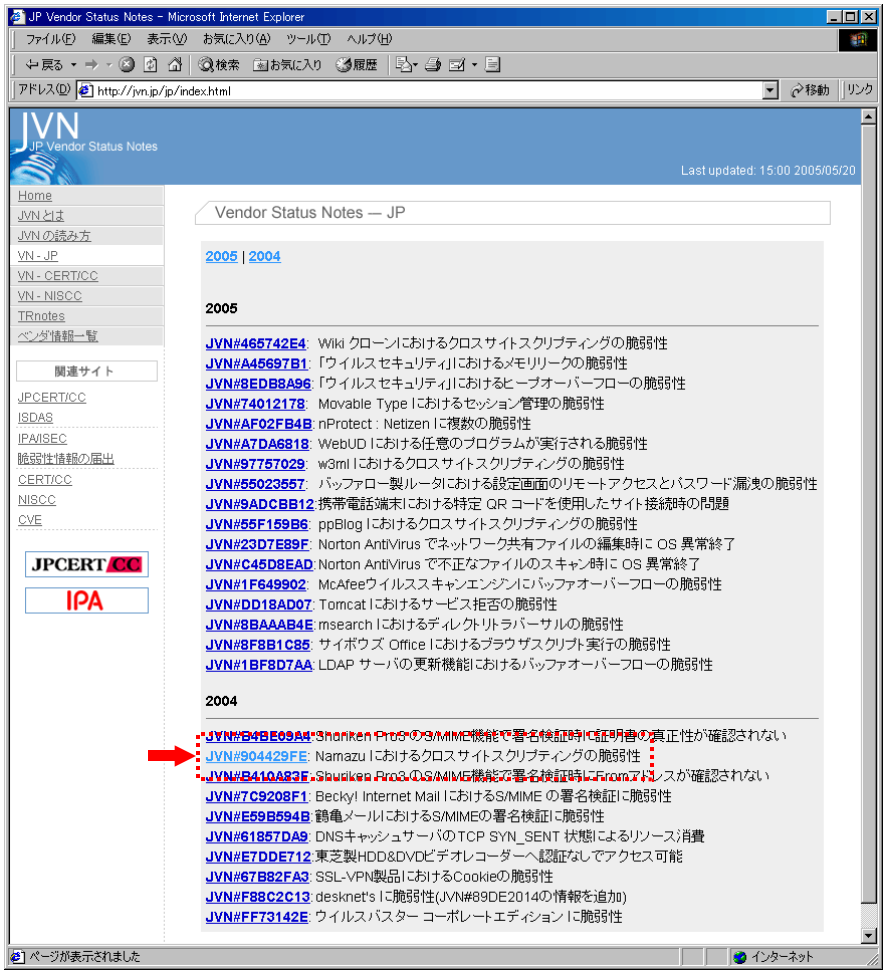
Namazu 2.0.13 に存在した脆弱性

- 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 2.0.14 のリリース



→ 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エア
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
NamazuProject
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/

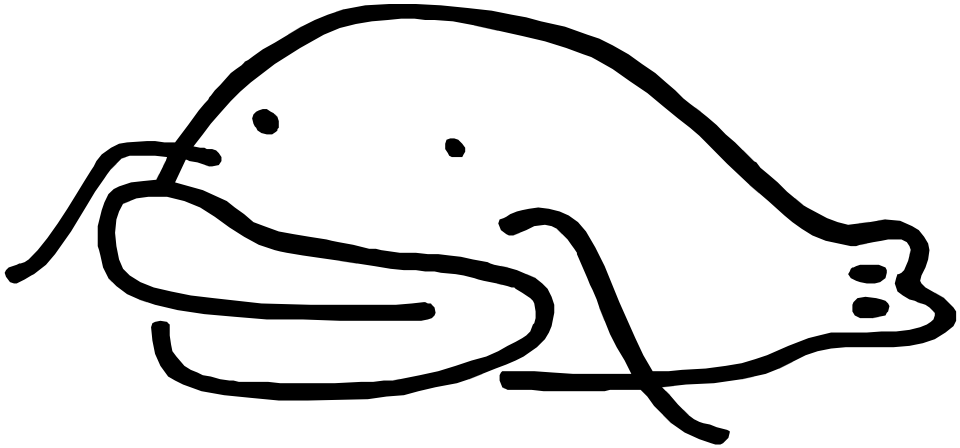
これまでの教訓(まとめ)

- 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@xxxxxxxxxx
- 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

Linux CONFERENCE 2005

Lightning Talk

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