JVNはFLOSSデベロッパを幸せにするか？

鈴木裕信

特定非営利活動法人フリーソフトウェアイニシアティブ

バックグラウンド

- ソフトウェア開発の世界にとびこんで約20年
  - UNIX、とくにBSDをやりたくて会社を選ぶ
  - 後にソフトウェア工学研究所へ
- フリーソフトウェア
  - 1985年末からGNU Emacsユーザ
- セキュリティ
  - 1991年ぐらいから
  - JPCERT/CCのブートアップから関係

経済産業省告示

- ソフトウェ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

JVN

- JPCERT/CCとIPAが共管で行っている脆弱性情報流通の枠組み
  - Japan Vulnerability Note
- IPA
  - 脆弱性情報のうけつけ
- JPCERT/CC
  - デベロッパとの窓口

デベロッパとの窓口

- デベロッパ対応
  - 脆弱性にコンタクト
  - 脆弱性対応の情報の受け取り

プロダクトラインに乗っているソフトウェア製品だと
5W1Hを準備することができる

開発形態は一定の
枠組みに入る

WHO	WHERE
WHAT	WHY
WHEN	HOW

FLOSSの開発形態

- 一人が中心となって開発している
- グループで開発している
  - チームを作って開発している
  - 緩やかな結びつきで開発が進んでいる

FLOSSの脆弱性対策の問題

- 一人が中心となって開発している
  - 誰が開発しているかわからない
  - その人が常にアクティブになっているわけではない

FLOSSの脆弱性対策の問題

- 緩やかな結びつきのグループで開発している
  - 中心のない持ち寄り型開発モデルの場合、コンタクト先を探す難しさ
    - しかし誰かは直してくれる
  - 脆弱性情報の管理をどうするか
    - 多数で共有するなら情報が漏れやすいだろう

FLOSSディストリビュート問題

- 修正版は公開されるだけではユーザに届かない
  - 流通ステップと開発者は独立した問題
- オンラインアップデート
  - ディストリビューションに依存する場合は、たぶん楽
  - 自分でコンパイルした場合は？

FLOSS開発者の懸念

- 負担の大きさ
  - 時間のプレッシャ
  - 世間からのプレッシャ
- 重箱の隅をつつき問題
  - 誰も使わないような機能までメンテナンスさせられる
- 脆弱性流通の手続きの複雑さ
  - NDA問題

やる気をそぐには十分なインパクト

- 一人で開発していると誰も相談できない
- 複数で開発していても誰がリーダーとなりJVNと対応していいかわからない

FLOSSデベロッパをサポートするには

- どういうJVNの運用がいいのか
- 誰がサポートしてあげるのか
- いったい誰が何をできるのか

情報システム等の脆弱性情報の取扱いに関する研究会

- 委員として参加
- 最終報告書2007.6
- FLOSSのソフトウェア脆弱性流通に対して（以前と比較した場合）柔軟な枠組を用意
- FLOSSコミュニティ側の多様性、自治性を尊重する形で進める必要性があることを会議では強調

コミットメント

- FLOSSコミュニティ側からコミットメントできる状況は作った
  - でもFLOSSコミュニティ側がコミットメントできないと、当然、元の黙阿弥

ここ2年のまとめとして

- ここ2年のまとめとしてFLOSSと脆弱性のシンポジュームを秋ぐらいから年末にかけてやりたい
  - FSIJ, JPCERT/CC, IPAのパネル討論

次の活動として

- セキュリティに関する情報・教育
  - JPCERT/CCやFSIJなどがFLOSS向けにするとよいかも
    - FLOSSデベロッパは必ずしも情報教育を受けているわけではない
    - 教育チャンスを増やす
- 情報制流通のHOW TOを示す
  - FLOSS向けのストーリーを示すと楽かも