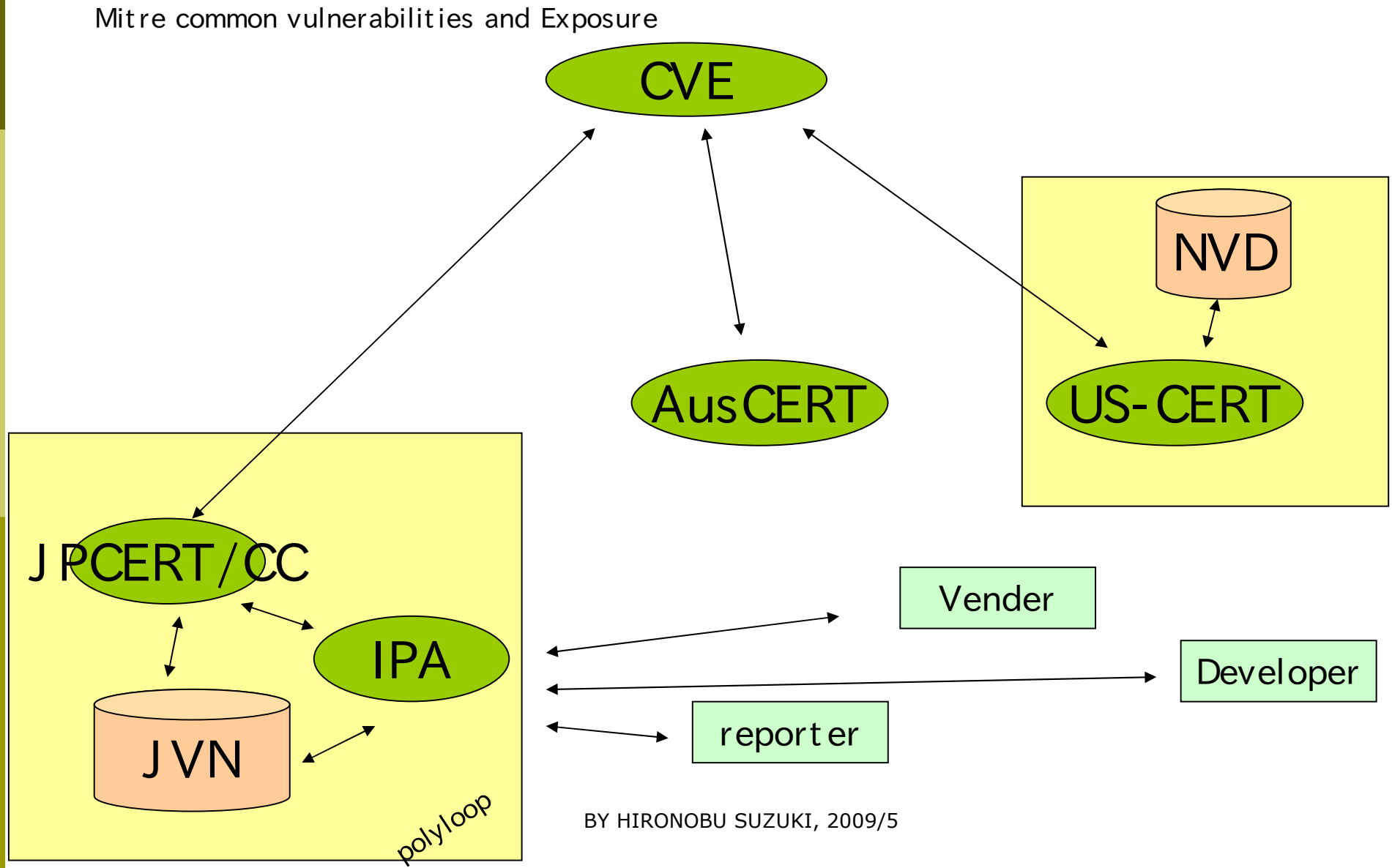
FLOSSの脆弱性情報流通

すずきひろのぶ

Process of Vulnerability Handing in General



国内で誰がFLOSS系は報告する？

- セキュリティ専門家
  - 彼らはツールを使ってチェックする
  - ツールの精度アップ用？
- 一般のひとは稀
- 報告は偏っている
  - Webアプリ系なのはツールがWebアプリ系に特化しているようだ

ＪVNが公開しているのは対応できたもの

- 企業がやっているオープンソースがターゲット
  - たぶん対応できるものだけ公開しているから
- 表に出ていないものは？
  - 実態はよくわかっていない

ケーススタディはむずかしい

- 企業として対応しているので
  - 一般の対応と同じで問題はない
- コミュニティで対応しているのは？
  - 結構もんだい
- 個人的に趣味でやっているのは？
  - とても問題
- ぜんぶ問題点・解決アプローチが違う

どうするべ？

- ステイブルな組織が継続的に中心になり
- コミュニティネットワークを作り
- 情報交換をし易く
- オープンソースのためのSecure Programmingを習得させる

Discussion

- IPA-JPCERT/CC-JVNをツールとして使うべし
  - これらの組織ができる活動は限られている
- ディストリビューションは影響範囲を知っている
  - 開発者だけじゃない
- 組み込んでいる周辺を含めるとかなり大きい
  - そこまで考えるとJVN公開以降も重要
- プラクティスを作って公開する
  - 参考にする・ディスカッションの元にできる