神話：OSSコミュニティは，クラッカーに負けない

植中 雄斗 (九州大学),
近藤 将成 (九州大学), 斎藤 忍, 飯村 結香子(NTT), 鵜林 尚靖, 亀井 靖高 (九州大学)

背景：リーナスの法則[1]

リーナスの法則

十分な数の開発者がいれば，全てのバグは直ちに発見，修正される

神話

OSSコミュニティでは
脆弱性は直ちに解決される

[1] Eric Raymond. The cathedral and the bazaar. Knowledge, Technology & Policy, 12(3):23–49, 1999.

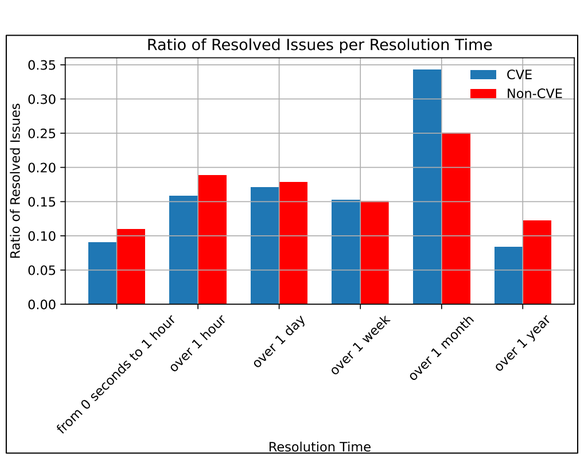
分析対象

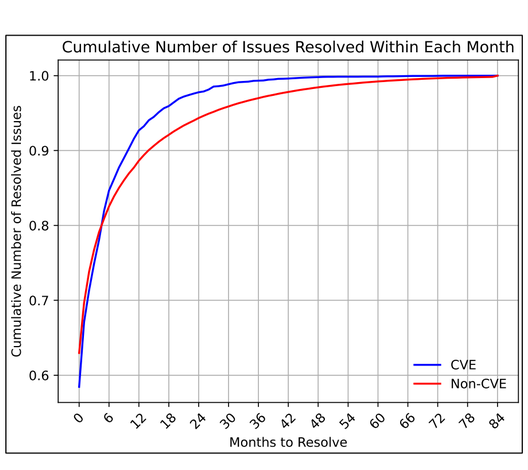
項目	値
リポジトリ数	225
総Issue数	1,227,442
脆弱性を扱うIssue数	7,465
脆弱性を扱わないIssue数	1,219,977
総PR数	1,525,604
脆弱性を扱うPR数	6,875
脆弱性を扱わないPR数	1,518,729

調査 1

脆弱性を扱うIssue，脆弱性を扱わないIssueのそれぞれで解決時間を調査.

解決時間 = Issueの解決日時 - Issueの作成日時





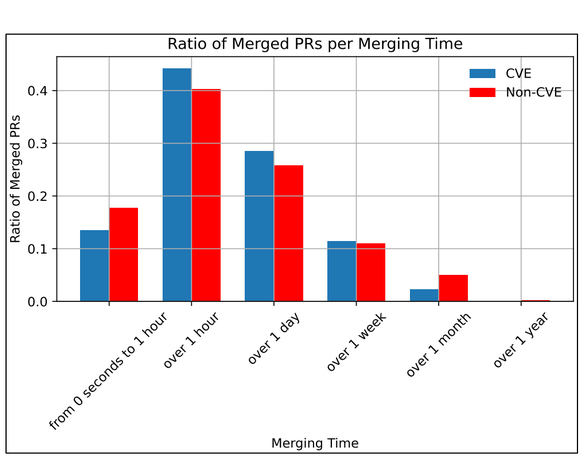
発見1-1：左図から，１年以内に解決されるIssueの割合は，脆弱性を扱うIssueの方が高い．右図からも，脆弱性を扱うIssueの方が比較的に解決時間が短いことが分かる.

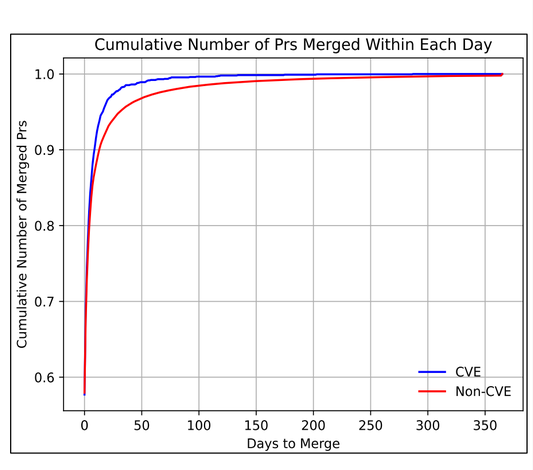
発見1-2：発見1-1に反して左図から，1日以内に解決されるIssueの割合は，脆弱性を扱わないIssueの方が高い.

調査 2

脆弱性を扱うPR，脆弱性を扱わないPRのそれぞれでマージ時間を調査.

マージ時間 = PRのマージ日時 - PRの作成日時





発見2-1：左図から，１ヶ月以内にマージされるPRの割合は，脆弱性を扱うPRの方が高い．右図からも，脆弱性を扱うPRの方が比較的にマージ時間が短いことが分かる.

発見2-2：発見2-1に反して左図から，1時間以内にマージされるPRの割合は，脆弱性を扱わないPRの方が高い.

事実，考察

OSSコミュニティでは
脆弱性は直ちに解決される

発見1-1,発見2-1の要因
- 開発者の脆弱性に対する意識が高い可能性

発見1-2,発見2-2の要因
- Issueの解決難易度
  - 脆弱性を扱うIssueは解決難易度が高い可能性
  - 脆弱性を扱わないIssueは極端に解決が簡単なものが多く含まれる可能性

追加の調査

- **脆弱性の重大度とIssueの解決時間の関連の調査**

仮説：開発者の脆弱性への感度が高いなら，開発者は重大度の高い脆弱性ほど優先的に解決を試みる.
結果：脆弱性の重大度と解決時間には相関がない.

- **Issue の解決時間とコメント数との関連の調査**

仮説：開発者の脆弱性への感度が高いなら，脆弱性を扱うIssue は議論が活発に行われる.
結果：脆弱性を扱わない Issue の方が議論が活発.

- **Issue と PR の包含関係の調査**

仮説：脆弱性は慎重に対応すべきであるため，IssueとPRの包含関係が守られる.
結果：13%の脆弱性でしか包含関係が守られない.