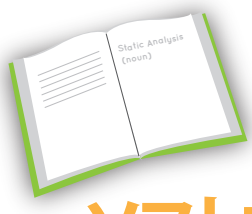
ソフトウェア開発者とって静的解析ツールが必要である理由

話は非常にシンプルです：セキュリティ上の脆弱性や深刻な欠陥のない、安全で信頼性の高いコードを作成しなければいけない場合、静的解析ツールはもはや必要不可欠です。



静的解析（または：ソースコード解析 ）は、プログラムを実行せずに、自動的にコンピュータソフトウェアの脆弱性を検出することができます。これにより開発者は、常にクリーンなコードをチェックインすることが可能になります。

ソフトウェアの欠陥＝

発売の遅れ＋リコール＋ブランドのダメージ ＋コスト＋深刻な損害

例

北アメリカにおける大停電

アメリカ東海岸の５５００万人もの人々が電気が使えない状態に

THERAC -25 放射線治療機器

患者に対して大量の放射線を照射する被害

アリアン5（ヨーロッパの使い捨て型ロケット）５０１便

3億7千万ドルのロケットが自爆

人手による欠陥の発見は非常に困難です

平均的なアプリケーションのセキュリティリスク件数

22.4件*

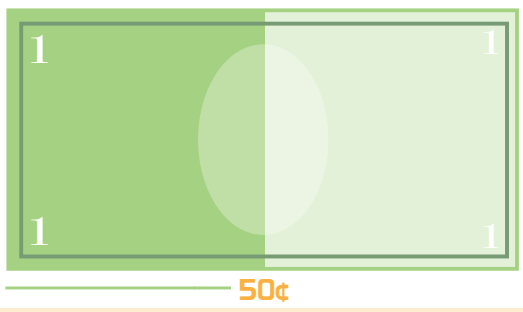
未満のバグ発見率

静的解析のようなツールやコードレビュープロセスが無い場合、プログラマーは、彼らのソフトウェアに潜むバグのうち、発見可能なのは全体のうちの***50%***未満です**

欠陥のコスト：

バグ修正のために世界中で毎年3120億ドル（約３０兆円）が費やされています***

開発およびメンテナンスの予算



ソフトウェアの開発およびメンテナンス費用の1ドルごとに、50セントはバグの発見および修正に費やされています。****

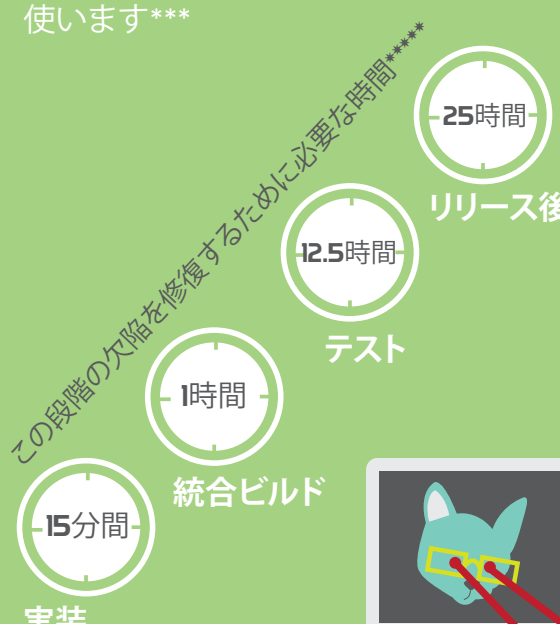
静的解析は、重大な脆弱性の発見や主要なコーディング基準の順守をお手伝いします

- バッファー オーバーフロー
- 非認証ユーザーの入力
- インジェクションの問題
- クロスサイトスクリプティング
- メモリーおよびリソースのリーク
- 並列処理違反
- NULLポインター間接参照
- 並列処理エラー
- エンディアンの非互換性
- 初期化されていないデータの使用

SAMATE / OWASP / CERT / MISRA / CWE™ / DISA STIGs / FDA / DO-178B / ISO-26262 / PCI

時間の節約

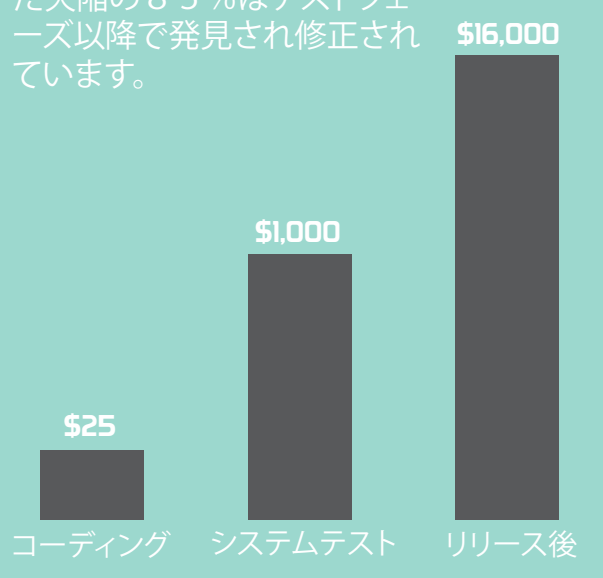
ソフトウェア開発者は、バグの発見および修正に、プログラミングの時間の半分を使います***



静的解析で早くバグを見つけ、時間を節約しましょう

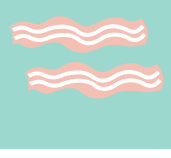
コストの節約

コーディング時に埋め込まれた欠陥の８５％はテストフェーズ以降で発見され修正されています。



16000ドル（約１５０万円）リリース後に見つかった欠陥*の修正に費やされた額*****

＝



ベーコンに換算すると約1600kg

クリーンなコード

✗ 従来のアプローチ

（収束しない欠陥）

コードを書きます
チェックインします
QAがバグを見つけます
コードを修正します
もう一度チェックインします
QAは、さらに多くのバグを見つけます

✓ 最新のアプローチ

（常にクリーンなコード）

コードを書きます
コーディング中にバグを修正します
クリーンなコードをチェックインします
より多くのコードを書きます

静的解析ツールにより、チェックイン前及びコーディング中にデスクトップで問題を修正することができます。

開発者：私にとっての利点は？

1. 従来のアプローチを止めることで、QAから報告されるバグ数を削減できます

2. 静的解析によって発見されるエラーから学ぶことによって、より良い開発者になれます

3. クリーンなコードをチェックインし、もっと重要な他の作業に時間を費やせます

4. 自分の書いたコードのバグが市場に流出してしまうことを防ぐことができます

開発マネージャー：私にとっての利点は？

1. 熟練開発者と新人開発者の差を狭めることが出来ます

2. 開発サイクルの早い段階で問題が解決されたことが確認出来、リスクが軽減出来ます

3. コードの欠陥に対処する時間を短縮することで生産性を向上させます

4. コードのセキュリティ、品質、複雑度のトラッキング、レポーティングによりソースコードを継続的に改善します

静的解析ツールで脆弱性のない高品質なコードに!

klocwork®

Klocworkは、オンザフライのソースコード分析ツールで、開発者がより安全で信頼性の高いソフトウェアを作成するお役に立ちます。

詳細、および無料トライアルの登録につきましては、以下をご覧ください。

www.klocwork.com/WhySCA

* 2013 Global Application Security Risk Report
https://www.aspectsecurity.com/uploads/downloads/2013/06/Aspect-2013-Global-AppSec-Risk-Report.pdf

** ケーパーズ・ジョーンズ、2012年
http://sqgne.org/presentations/2012-13/Jones-Sep-2012.pdf

*** ケンブリッジ大学Study States Software Bugs Cost Economy $312 Billion Per Year
http://markets.financialcontent.com/stocks/news/read/23147130/Cambridge_University_Study_States_Software_Bugs_Cost_Economy_$312_Billion_Per_Year

**** ケーパーズ・ジョーンズ、2012年
http://www.ifpug.org/Documents/Jones-SoftwareDefectOriginsAndRemovalMethodsDraft5.pdf

*****応用ソフトウェア測定、ケーパーズ・ジョーンズ、1995年