

Code Dx

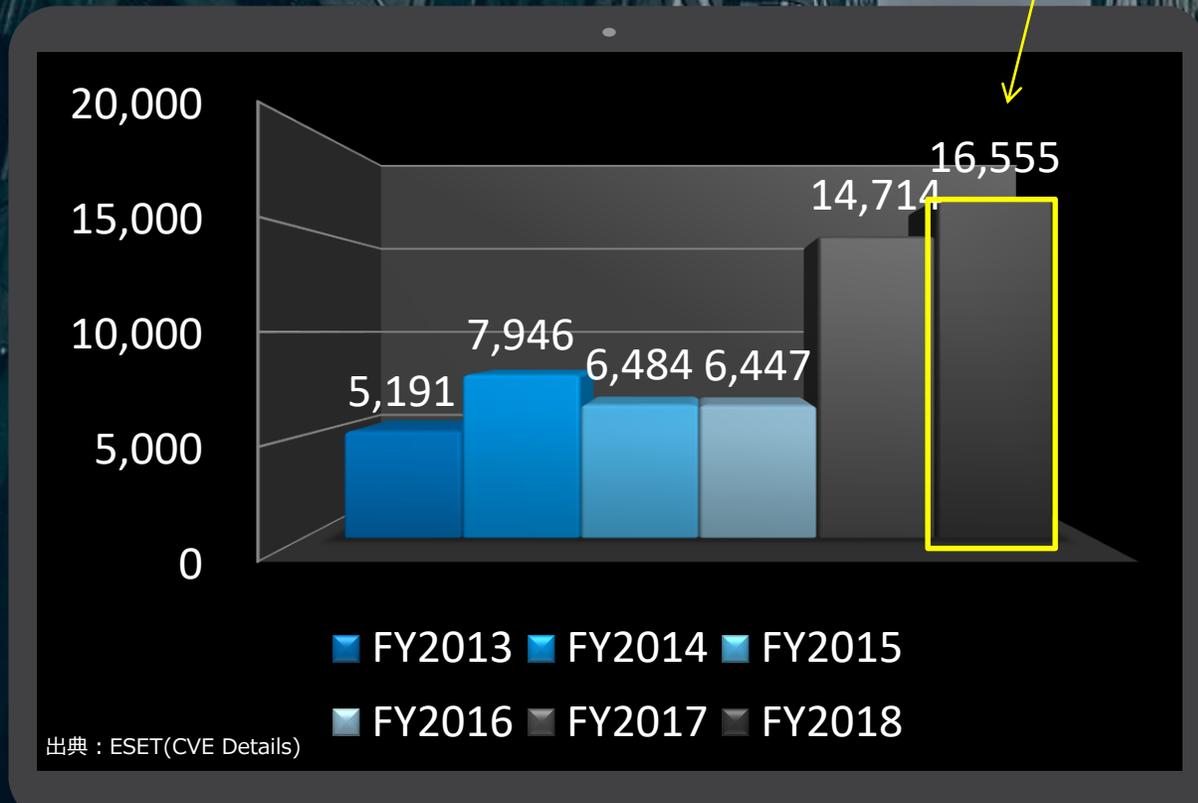
ソフトウェアの品質と 脆弱性の管理ツール

リスク分析作業期間を劇的に短縮

2019年1月24日
株式会社ガイア・システム・ソリューション
営業統括部 岡崎 幹夫

ソフトウェア脆弱性の現状： 脆弱性の報告件数は急激に増加中

2018年 過去最高

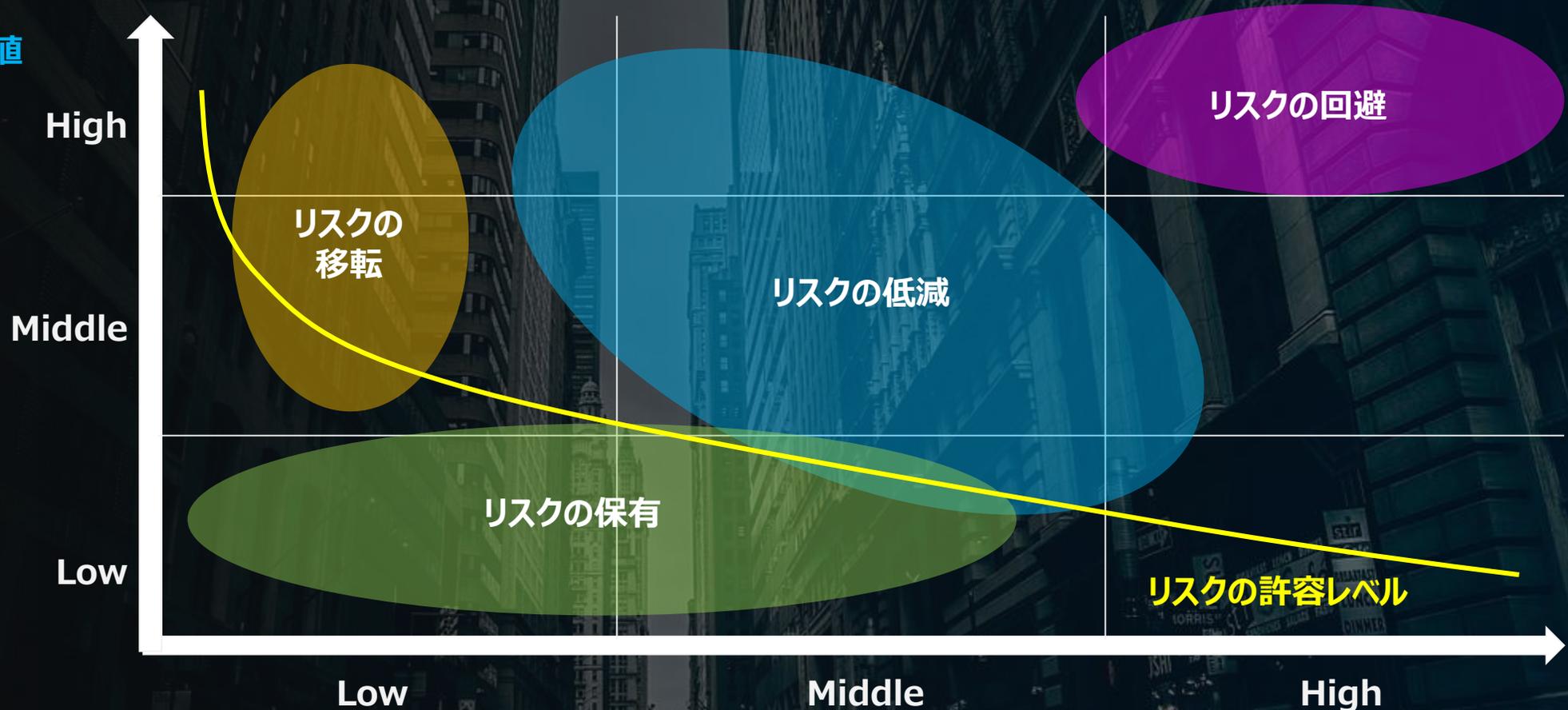


Cross Site Scripting (XSS)
SQL Injection
Code Execution
Overflow
Dead Code
DoS

対策：リスクアセスメントが必要

情報収集、整理、リスク分析で、リスクを明確化

リスク発生の際の損害の大きさ
(影響度)
= 情報資産の価値



引用：情報処理推進機構（IPA） 情報セキュリティマネジメント概念図より

リスクの発生可能性
= (脅威 × 脆弱性)

課題 1 : 脆弱性検証ツールの限界

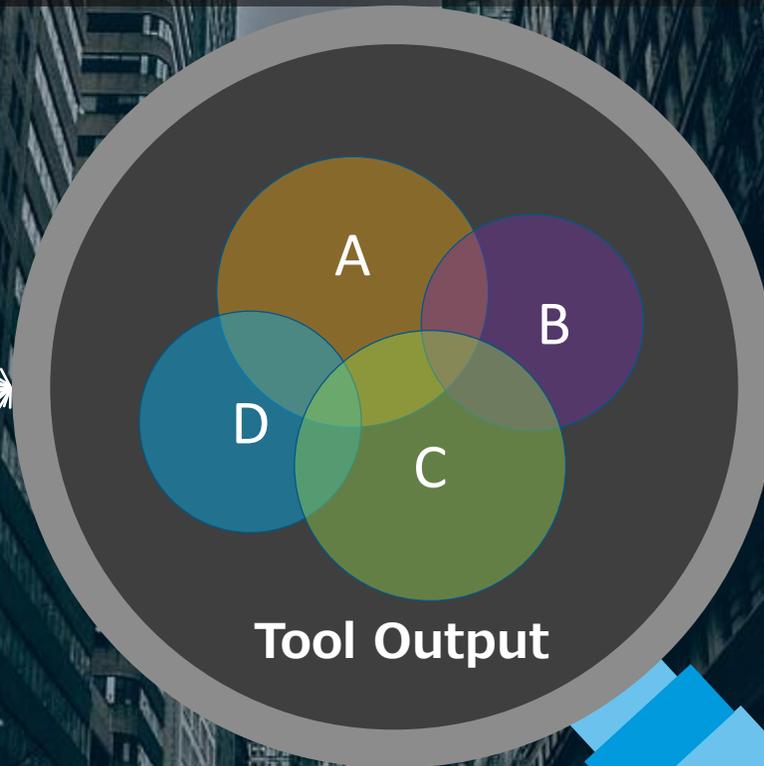
1つのツールだけで全ての脆弱性は見つけれない

ツールA

ツールB

ツールC

ツールD



ツール毎に、
強み/弱みがあるので、
複数ツールを使用する

平均的な1つの
静的分析ツールは、
すべての脆弱性の

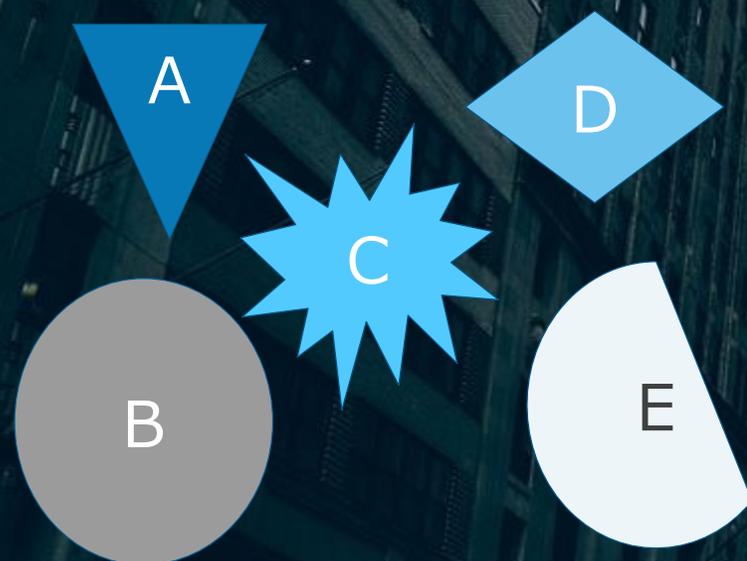
14%

しか検出しない

出典 : Kris Britton and Chuck Willis, "Sticking to the Facts:
Scientific Study of Static Analysis Tools", Sept 2011:
<http://vimeo.com/32421617>

課題 2 : 複数ツール使用時の問題

ツール毎に異なる結果の正規化と、相関は難しい

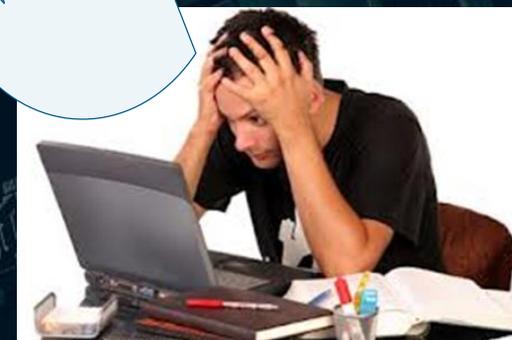
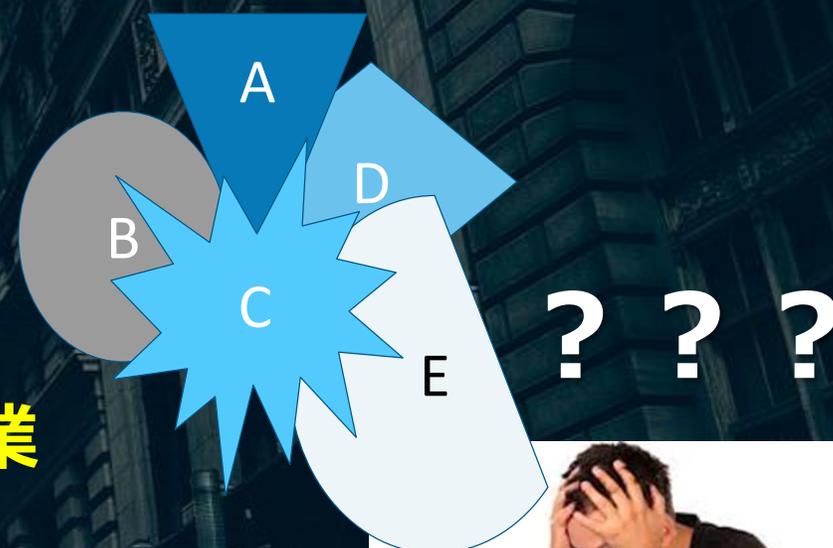


Tool Output

書式、構文、命名は
全てユニークで異なる

手作業

数日～数週間の作業



Solution : Code Dxが、脆弱性リスク分析の問題を全て解決



複数の検証ツール結果を
まとめて取込み、
脆弱性リスク分析の為の
正規化と相関を自動で行い、
**1つの解析結果を数分で、
自動生成します。**

数日～数週間
の作業



数分

Code Dxサポートツール/言語/業界標準一覧

DAST/IAST



Software Composition Analysis



Other Tools



SAST



Plugins



Languages



Standards and Compliance Mapping



THANK YOU.

CodeDx

 GAIA System Solutions Inc.