

# スマートアグリゲーションがもたらす 高品質検証手法

2019年12月3日  
株式会社イーエルティ

チーフコンサルタント 落井 裕治

# Code Dx

## Code Dx概要

 **Department of Homeland Security**  
(DHS: 米国国土安全保障省)

2001年9月11日に発生したテロを踏まえ、2012年11月に設置  
公共の安寧の保持を所管。ESTAなどを発行。

AppSec  
R&D



DHSとの研究成果  
を持って、2015年に  
Secure Decisions  
からスピナウト

ブート  
ストラップの  
資金提供

DHSと継続  
される  
AppSec  
R&D成果



※1 AppSec  
= Application Security

DHS (<https://www.dhs.gov/>)

Applied Visions, Inc. (<https://www.avi.com/>)

Secure Decisions (<https://securedecisions.com/>)

Code Dx, Inc. (<https://codedx.com/>)

## Code Dx, Inc.

- 本社： New York
- Applied Visions, Inc.には、米国政府のサイバーセキュリティ研究を専門とする部門 Secure Decisionsがあります。
- 同部門は**米国国土安全保障省（DHS）科学技術局の資金提供を受け、アプリケーションコードが安全であることを保証するソフトウェアの研究開発**を行いました。
- 米国政府のソフトウェアサプライチェーンを確保するため、規制や業界のベストプラクティスに準拠しています。
- 他の資金提供も受け、Secure Decisionsは最終的に製品「Code Dx」（「Dx」は「診断」の医療表記です）になったテクノロジーを開発し独立した会社を設立。
- Code Dxは、静的コード分析のプラットフォームとして開始されました。Code Dxは、動的テストツールのサポートを追加することで、ハイブリッド分析の脆弱性スキャナになりました。
- 継続されているDHSとSecure Decisionsの研究結果は、Code Dxの改良に利用されています。



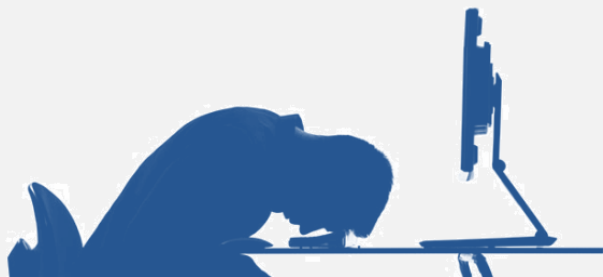
## Customers



※日本国内の顧客は除く

## ● 課題：品質とセキュリティのテストがリソースを大量に消費する

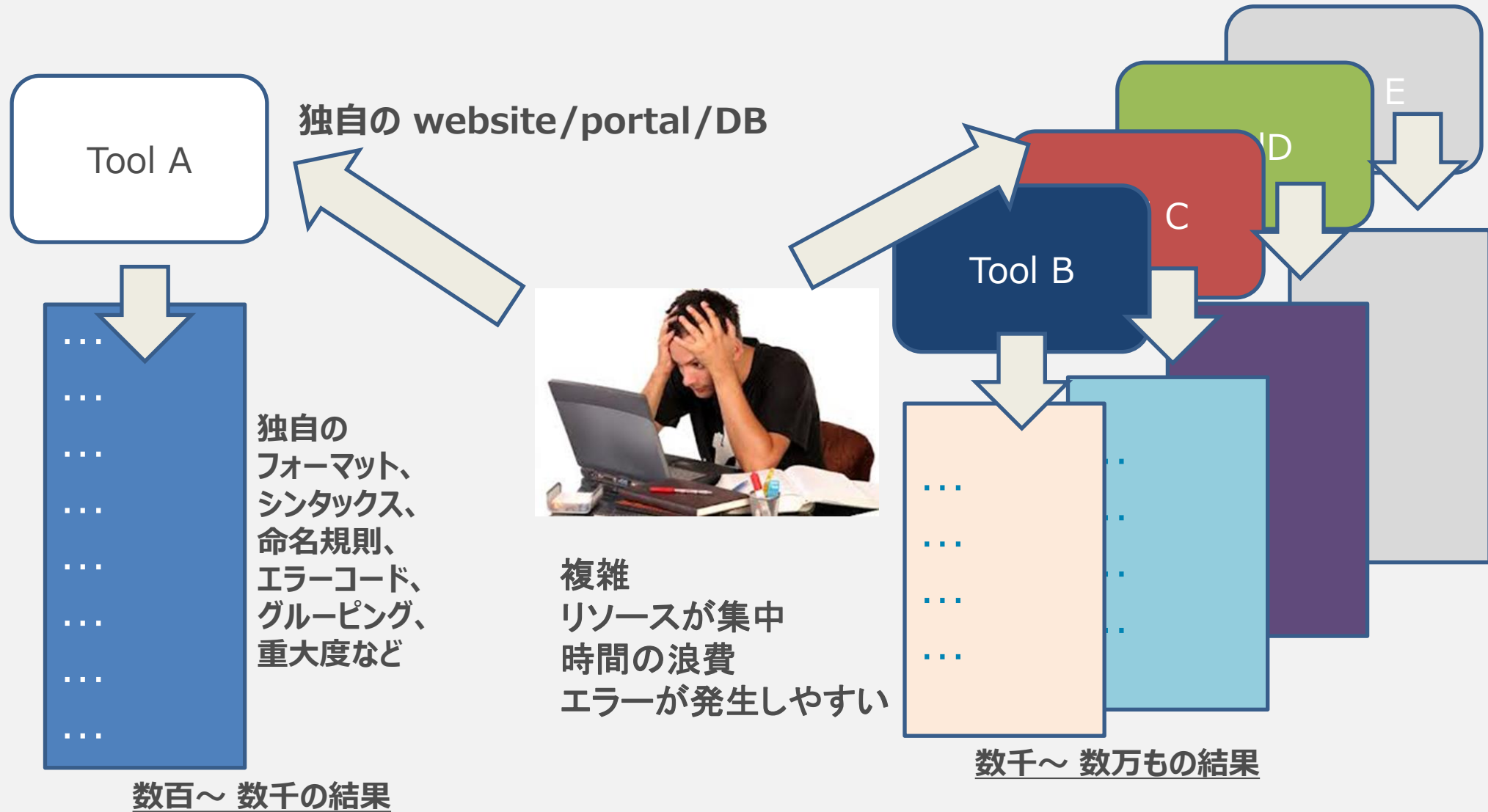
- マニュアルコードレビューは時間がかかり、包括的ではない。
  - ◆ 既存の静的および動的解析ツール（商用およびオープンソース）は数多く存在するが、それらは複雑で管理が難しい。
- 1つのツールですべてを見つけることはできない。<sup>※1</sup>
  - ◆ カバレッジを向上させ、可能な限り多くの問題を見つけるためには、**複数のツールを実行する**必要があり、その後、**結果を手動で組み合わせる**必要がある。
  - ◆ ツールは、**非常に大量のデータを生成**し、このデータは、最も重要な問題が特定され、最初に対処されるように、**レビュー、理解、優先順位付け**が必要。
  - ◆ アプリケーションに欠陥やセキュリティ上の脆弱性がないことを保証するのは、時間がかかり、コストがかかる。しかし、それは**必要**であり、そして非常に**重要**。



MISRAコンプライアンス  
構想 後半で～

※1

NSA Center for Assured Software, Kris Britton and Chuck Willis,  
“Sticking to the Facts: Scientific Study of Static Analysis Tools”, Sept 2011  
(<http://vimeo.com/32421617>)



## 手動

- スプレッドシートまたはその他のカスタムレポートを使用
- リソース集約型
- エラーを起こしやすい
- 数日または数週間かかることがある



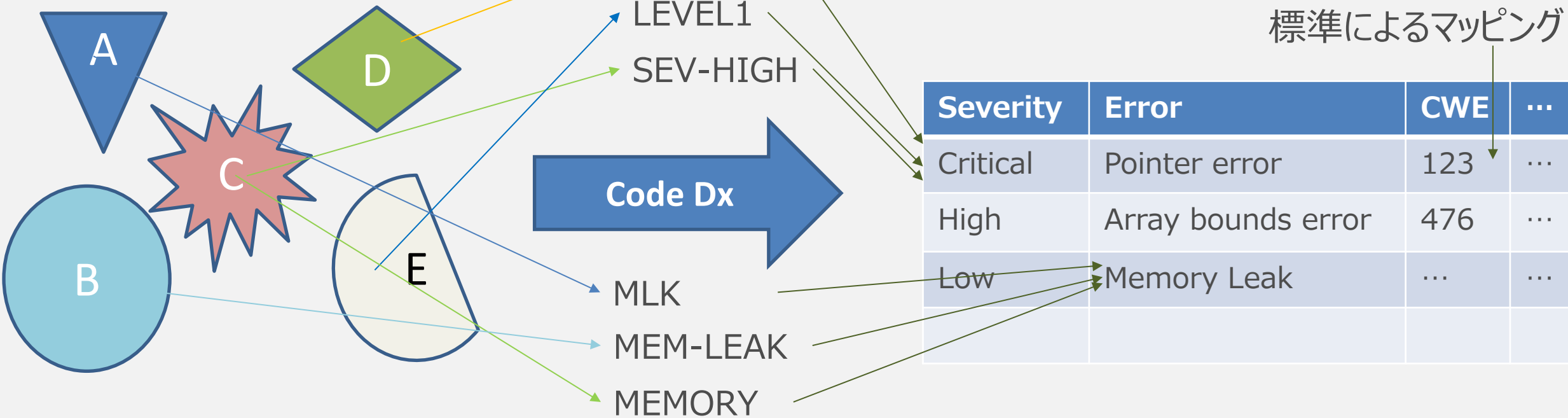
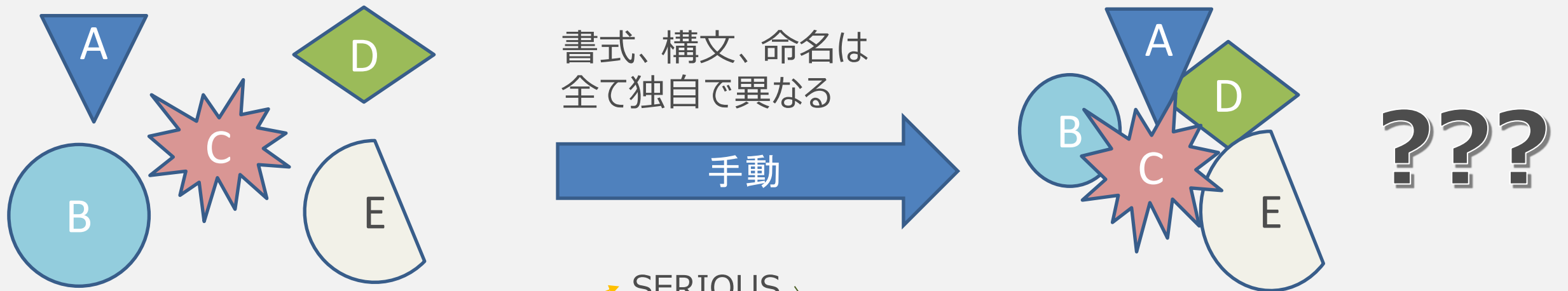
各ツールには、様々なレポートメカニズム、さまざまな形式、異なるシンタックスがある

## 自動

- アプリケーションを使用
- 問題の相関システム
- 一貫性と信頼性
- 数分程度で終了

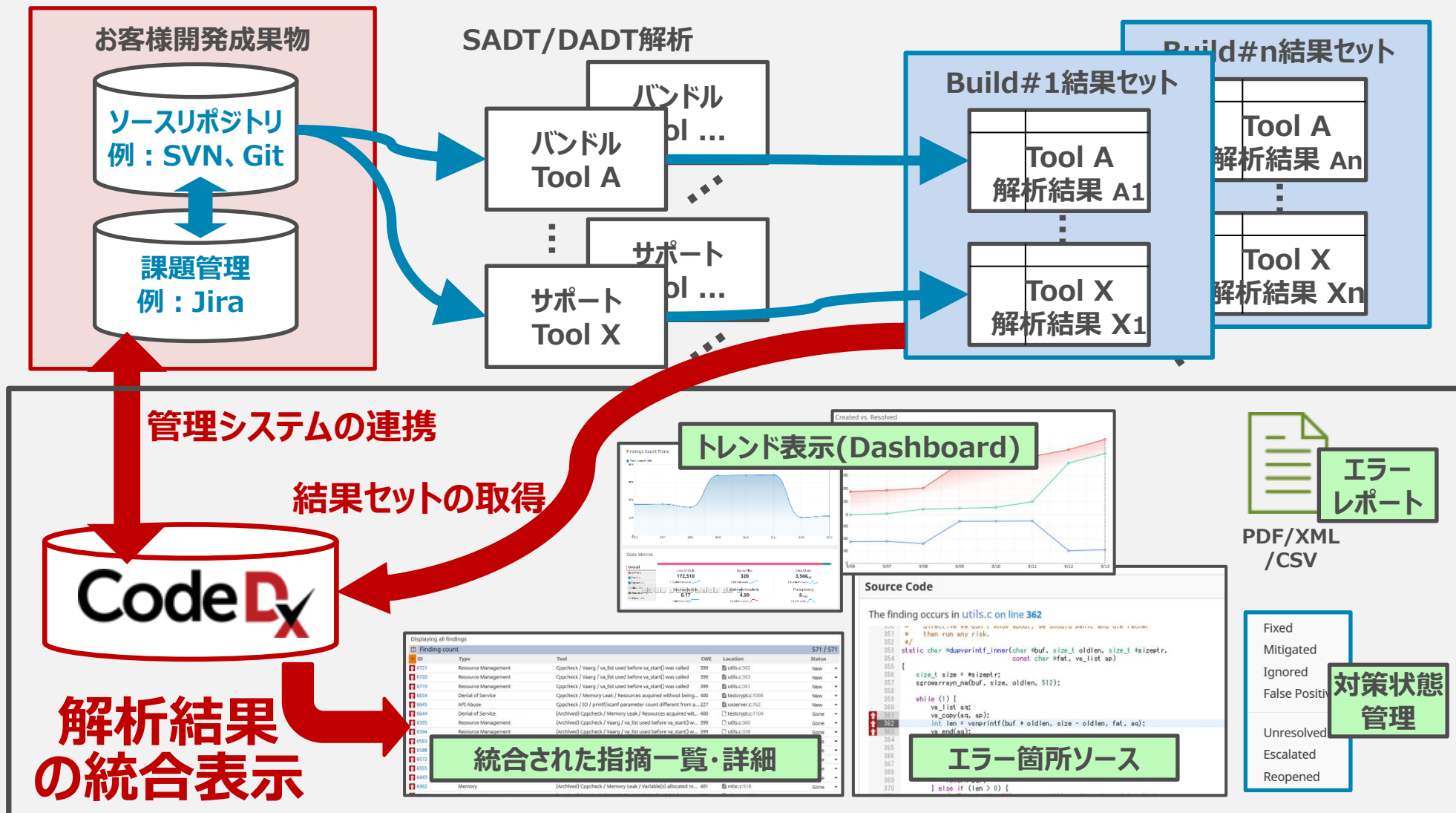


Code Dxは、CWEを比較のための共通指標として使う事で、オープンソースツールを有用なものにします。



- **静的解析の結果をプロジェクト単位で俯瞰できます**⇒ダッシュボード
  - 問題点（エラー）指摘のカウン트의トレンドを一望（バージョンアップや、比較的大きな変更の前後の状況を一目で確認）
  - 脆弱性やルール遵守に関する大きな問題の早期発見⇒早期の対策を実施可能
  - プロジェクト内の管理上の問題の推定⇒対策遅れや問題の傾向の発見と対策（問題解決までの日数、発生vs対策の傾向）
- **問題点（エラー）の一覧画面を、複数観点で確認し・状況把握が可能です**
  - ツール別、重要度別、ソースファイル別、対策までの時間別、前回の変更・対策からの時間別等
  - 複数のツールで検出した問題点への絞り込み⇒重点対策の判断に貢献
  - MISRA、CWE等のルール別の問題点把握⇒開発チーム、プロジェクト単位での大きな問題点の把握と対策
  - 問題点のステータス別の状況把握⇒個々の進捗はもちろん、組織としての対応状況の把握と対策に貢献（複雑な問題の後回し、スキル不足等の把握と対策検討）
- お客様のビルド環境や、独自ツールのデータをツールで取得(別途個別に対応)

# CodeDxによる、複数ツール解析結果の統合



## ボトムアップの品質向上



高速化の為に、  
(1)ビルド・テストを**自動化&高速化**し、早く成果を共有  
(2)状況把握・的確な判断に役立つ**透明性ある情報の共有**

リリース/  
Deploy

開発ルール遵守強化を支援

Code Dx  
による  
脆弱性対策

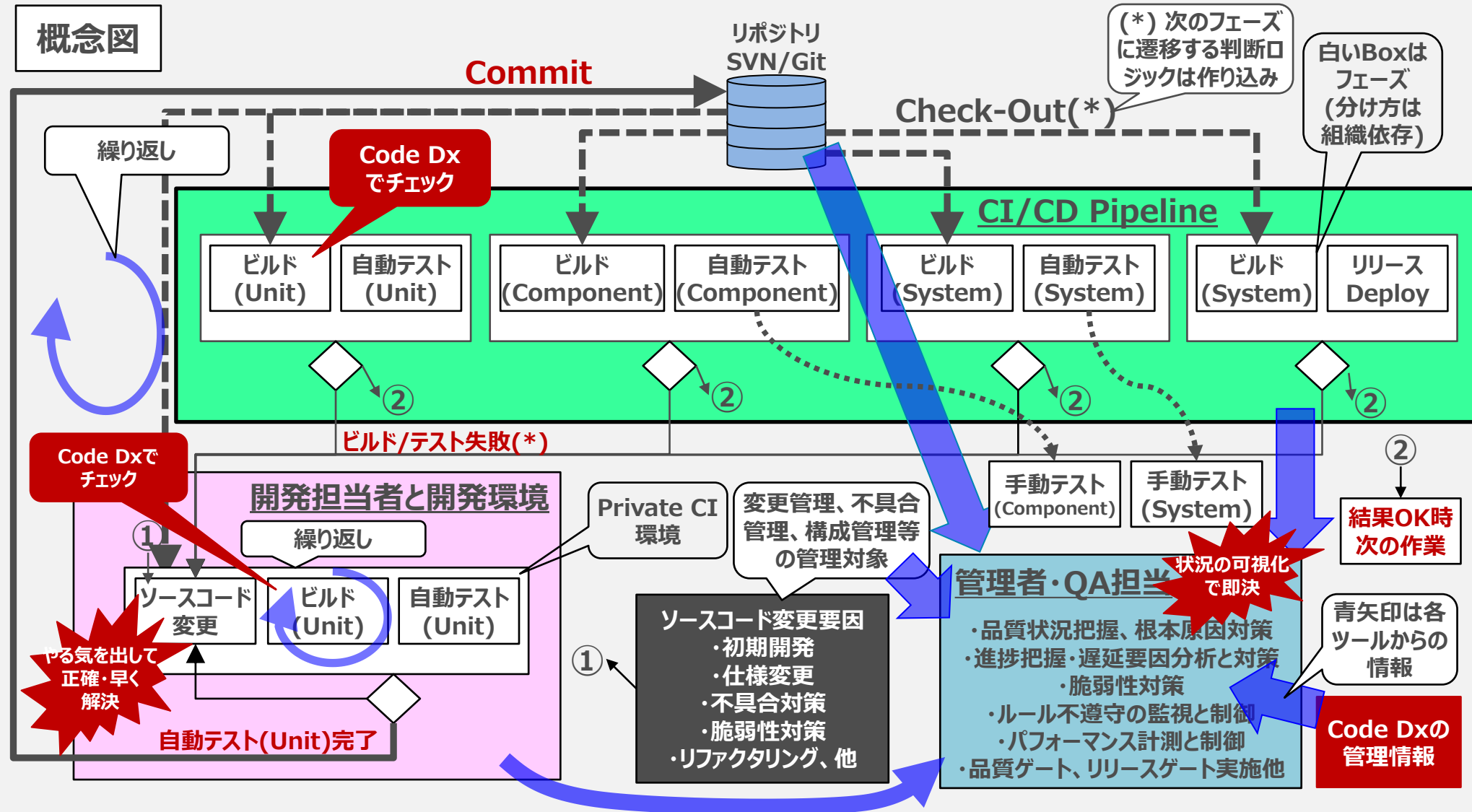
新規開発、派生開発

既存開発分、開発母体

コーディングルールの厳格化と遵守&  
修正Unit単位でチェック&対策(短時間)

システム全体で、修正範囲や優先度を決めて、  
開発計画に織り込む(中長期計画)  
実施は開発担当者(個々の修正は短時間)

・大量の検出結果を自動分類し、計画策定支援  
・対策状態を可視化し管理徹底  
・複数ツールの組合せで検出精度を向上



- Code Dxは、コードを品質及びセキュリティ問題の視点で分析する、オープンソフトウェアツール群を自動的に選択し、設定し、実行します。  
(サードパーティ製コンポーネントのステータスチェックも含まれます)

結果：開発者、テスター、QA / QCの時間を大幅に削減します。

- 複数の分析（静的および動的）ツール、または手動テストおよびレビュー結果によって検出された問題を相関させ、正規化し、重複を排除し、すべての結果を単一のデータセットに統合します。

結果：異なるツールの結果を集計する時間を数週間節約できます。

- 修復の特定、優先順位付け、追跡の管理プロセスを効率化します。

- ビジュアル分析とフィルタリングにより、問題の優先順位付け
- CERT、CWE、HIPAA、PCI、DISA STIGおよび他の業界標準へのマッピング
- 修復を加速するためのソースコードへのリンク
- 開発環境およびissue/problem/Bug追跡システムとの統合



**Code Dx:**  
品質・セキュリティ向上を支援

# サポート済みのSAST/DAST/IAST他ツール



## オープンソースツール

Category	Tool	Type	Focus
Open Source	Android Studio Lint	Static Analysis	Quality/Security
Open Source	Arachni	Dynamic Analysis	Security
Open Source(*1)	Brakeman	Static Analysis	Security
Commercial	CAT.NET (Microsoft)	Static Analysis	Security
Open Source(*1)	CheckStyle	Static Analysis	Standards
Open Source	Clang	Static Analysis	Quality
Open Source	CodePeer (AdaCore)	Static Analysis	Quality/Security
Open Source(*1)	CppCheck	Static Analysis	Quality
Open Source	Error Prone	Static Analysis	Quality
Open Source(*1)	ESLint	Static Analysis	Quality
Open Source	Find Bugs	Static Analysis	Quality
Open Source(*1)	Find Security Bugs	Static Analysis	Security
Commercial	FxCop (Microsoft)	Static Analysis	Quality/Security
Open Source(*1)	Gendarme (Mono Project)	Static Analysis	Quality
Open Source	GoLang Errcheck	Static Analysis	Quality
Open Source	GoLang Go vet	Static Analysis	Quality
Open Source	GoLang Gocyclo	Static Analysis	Quality
Open Source	GoLang Golint	Static Analysis	Quality
Open Source	GoLang Gosec	Static Analysis	Security
Open Source	GoLang Ineffassign	Static Analysis	Quality
Open Source	GoLang Safe SQL	Static Analysis	Quality
Open Source	GoLang Staticcheck	Static Analysis	Quality
Open Source	JLint	Static Analysis	Quality
Open Source(*1)	JSHint	Static Analysis	Quality/Standards
Open Source	OCLint	Static Analysis	Quality
Open Source(*1)	OWASP Dependency-Check	Component	Security
Open Source	OWASP ZAP	Dynamic Analysis	Security
Open Source(*1)	PHP_CodeSniffer (pear)	Static Analysis	Standards
Open Source(*1)	PHP_Mess Detector	Static Analysis	Quality
Open Source(*1)	PMD	Static Analysis	Quality
Open Source(*1)	Pylint	Static Analysis	Quality
Open Source(*1)	Retire.js	Static Analysis	Security
Open Source	Retire.js	Component	Security
Open Source(*1)	Scalastyle	Static Analysis	Quality/Standards
Open Source	SonarQube	Static Analysis	Quality
Open Source(*1)	SpotBugs	Static Analysis	Quality

\*1 CodeDx Enterprise にバンドル済み

## 商用ツール

Category	Tool	Type	Focus
Commercial	Acunetix	Dynamic Analysis	Security
Commercial	AppScan (HCL)	Static Analysis	Security
Commercial	App Spider (RAPID7)	Dynamic Analysis	Security
Commercial	ASoC (IBM->HCL)	Dynamic Analysis	Security
Commercial	BlackDuck (Synopsys)	Component	Security
Commercial	Burp Suite	Dynamic Analysis	Security
Commercial	Checkmarx	Static Analysis	Security
Commercial	CodeSonar (GramaTech)	Static Analysis	Quality/Security/Standards
Commercial	CONTRAST Assess	Dynamic Analysis	Security
Commercial	Coverity (Synopsys)	Static Analysis	Quality/Security/Standards
Commercial	C++Test (Parasoft)	Static Analysis	Quality/Security/Standards
Commercial	dotTest (Parasoft)	Static Analysis	Quality/Security/Standards
Commercial	Fortify Static Code Analysis	Static Analysis	Security
Commercial	Fortify WebInspect	Dynamic Analysis	Security
Commercial	Jtest (Parasoft)	Static Analysis	Quality/Security/Standards
Commercial	Nessus (tenable)	Net Security	Security
Commercial	NetSparker	Dynamic Analysis	Security
Commercial	NMAP Security Scanner	Net Security	Security
Commercial	Now Secure	Static Analysis	Security
Commercial	Protecode SC (Synopsys)	Component	Security
Commercial	Seeker (Synopsys)	Interactive	Security
Commercial	Sonatype Nexus	Component	Security
Commercial	Trustwave App Scanner	Dynamic Analysis	Security
Commercial	BJVFHTIJ	Static Analysis	Security
Commercial	Veracode Software CA	Component	Security
Commercial	Vex (UB Secure)	Dynamic Analysis	Security
Commercial	VM (Qualys)	Net Security	Security
Commercial	WAS (Qualys)	Dynamic Analysis	Security
Commercial	WhiteHat Sentinel Source	Static Analysis	Security
Commercial	WhiteHat Sentinel Dynamic	Dynamic Analysis	Security
Commercial(*2)	Embold	Static Analysis	Quality/Security
Commercial(*2)	Klocwork	Static Analysis	Quality/Security
Commercial(*2)	Lattix	Static Analysis	Architecture
Commercial(*2)	PGReleaf	Static Analysis	Quality/Security
Commercial(*3)	Polyspace	Static Analysis	Quality
Commercial(*2)	QA - C	Static Analysis	Quality/Security
Commercial(*2)	Sparrow	Static Analysis	Quality/Security

\*2 サードパーティによってカスタム統合済み。

\*3 統合予定

(2019年10月現在)

## Code Dx デモをご覧ください

- 基本の画面のご紹介
- 簡単なプロジェクトの解析と結果表示

## MISRAコンプライアンス ツール構想

よく聞かれます：コンプライアンス？何を示せば良いの？

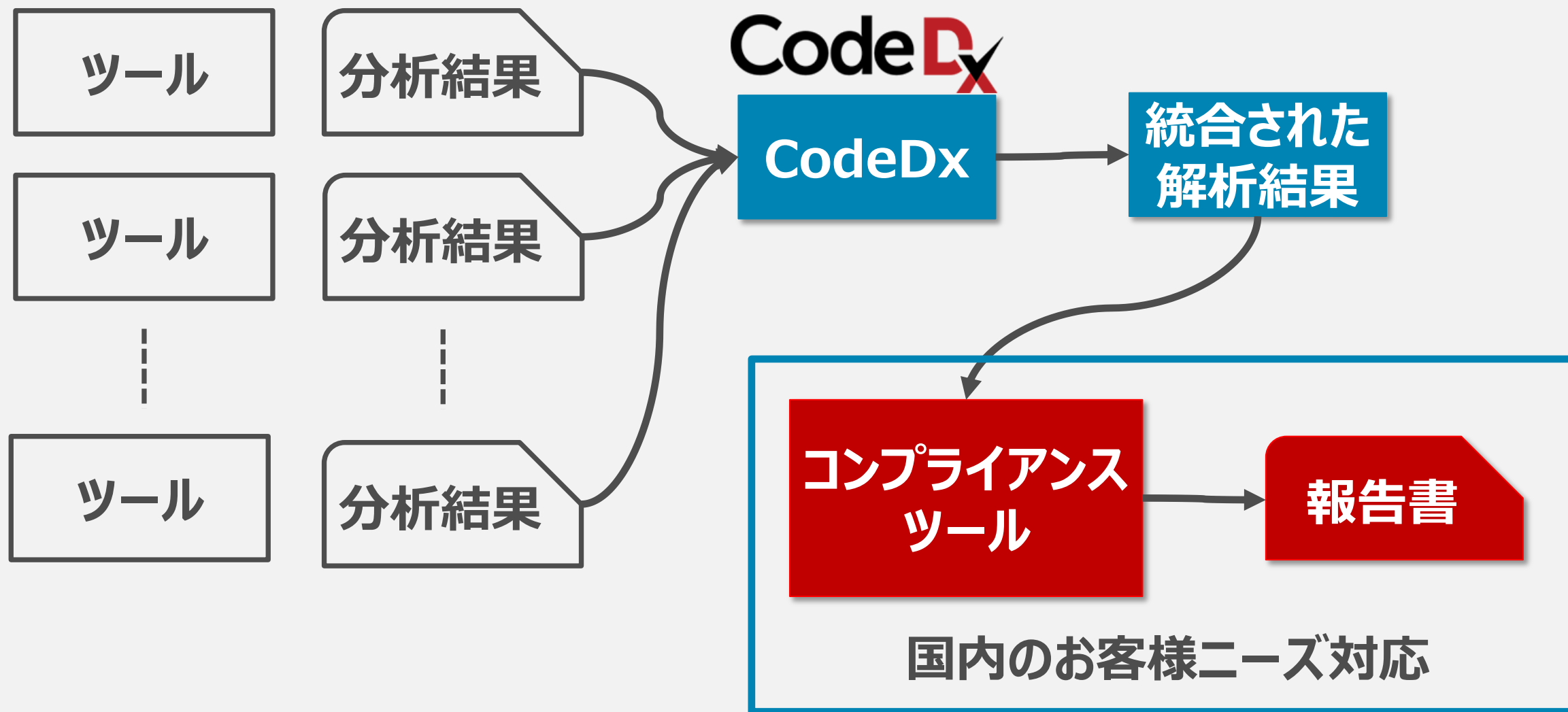
以下の事を示す必要がある

- 適用した**ガイドライン**
- **実施手法**の有効性
- どんな**逸脱**（Deviation）があったか
- 統制の取れた**開発プロセス**
- **プロジェクト外で開発されたコンポーネント**の状態



Code Dxを活用して  
エビデンス（報告書）  
作成支援

MISRA Compliance 2016(April 2016)



CodeDx

CodeDx

統合された  
解析結果

コンプライアン  
スツール

## 報告書作成支援

実施計画

カテゴリ変  
更計画

逸脱の  
定義・承認

コンプライ  
アンスサマリ

- 解析結果と正確に連動
- 複数ツール結果活用
- 作成工数・期間削減
- MISRAをターゲット

ご静聴ありがとうございました