システム開発における アプリケーションセキュリティ 3つのポイント

株式会社オージス総研
サービス事業本部アプリケーションセキュリティソリューション部
早苗 朋宏

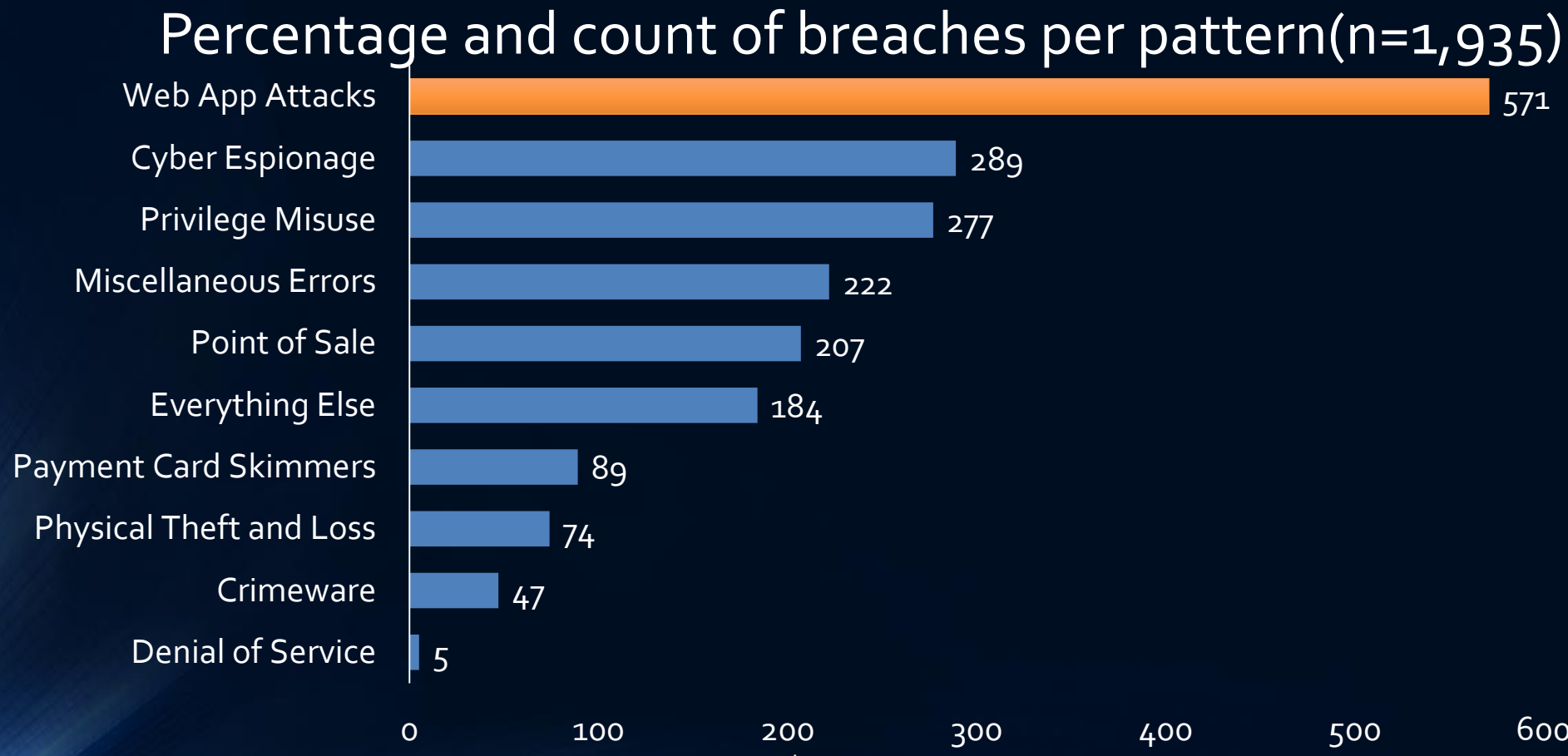
オージス総研

本日の範囲

- 物理 ・・・・・・・・・・入退室管理
- ネットワーク ・・・・・・・・・・F/W,IDS,IPS,WAF
- ホスト ・・・・・・・・・・OS設定
- アプリケーション ・・・・・・・・・・【本日の範囲】
- データ ・・・・・・・・・・暗号化

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

データ侵害の多くは、Webアプリケーションに対する攻撃で起きている



Verizon 2017 Data Breach Investigations Report 10th Edition https://www.verizonenterprise.com/jp/DBIR/2017/

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

アプリケーションセキュリティ３つのポイント

① よりどころとなる指標を持つ

② 具体的な活動を決める

③ すみずみまで何度も繰り返す

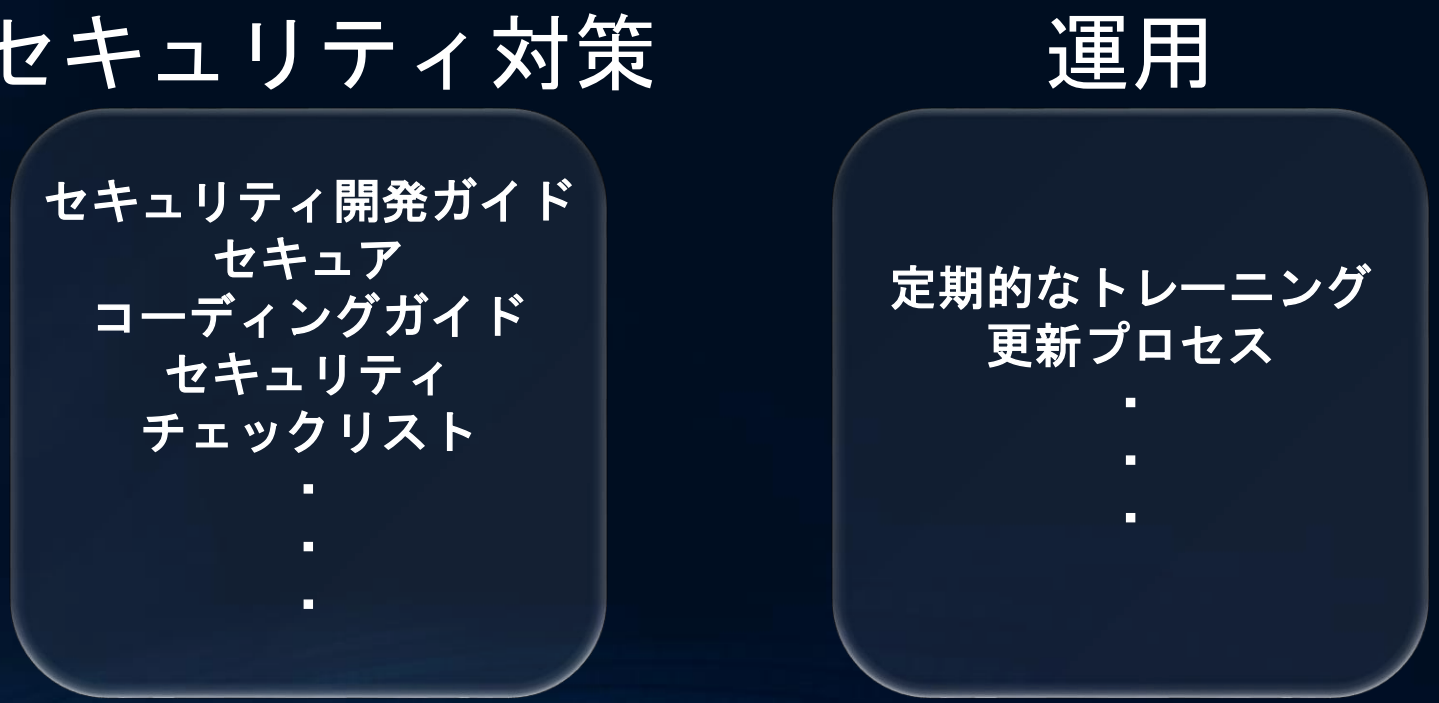
Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

① よりどころとなる指標を持つ

自社の**アプリケーション**に関するセキュリティ対策の現状についてどのように把握されていますか？

現状把握

どんなセキュリティ対策をアプリケーションに対し、行い、どのように運用しているか？



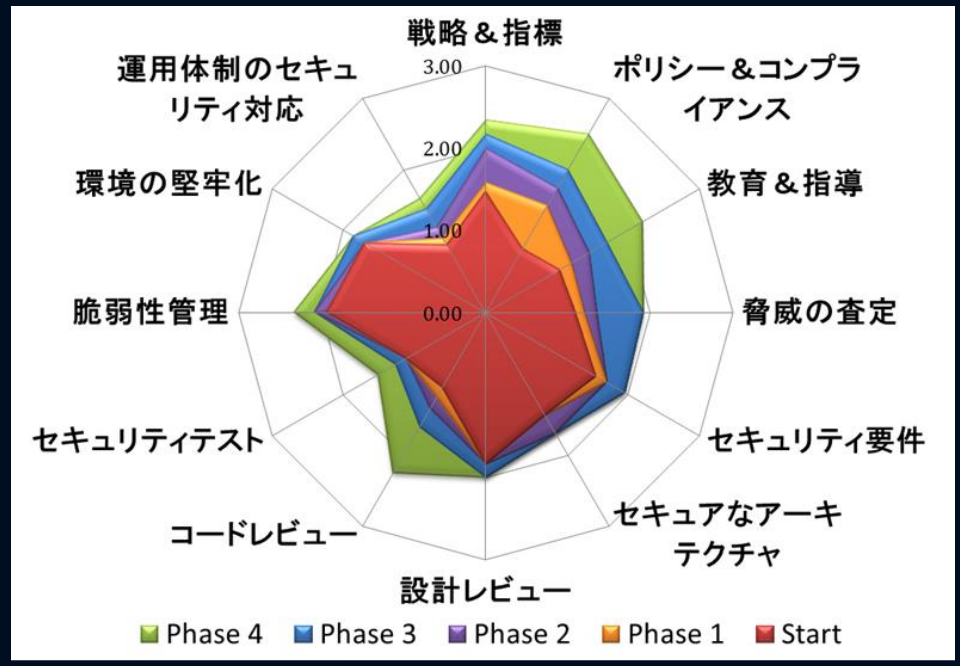
Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

現状の対策で
十分でしょうか？

グローバルな指標を使う

OpenSAMM

77の設問を通じてソフトウェアのセキュリティ保証に関する成熟度を12のアクティビティ別に3段階で可視化



＜特長＞

・セキュリティ保証成熟度の評価
　⇒　可視化

・セキュリティ保護体制の強化指標例示
　⇒ ロードマップの作成

参照：
https://www.owasp.org/index.php/OWASP_SAMM_Project

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

OWASP

Open Web Application Security Project

弊社は、ローカルチャプタースポンサー

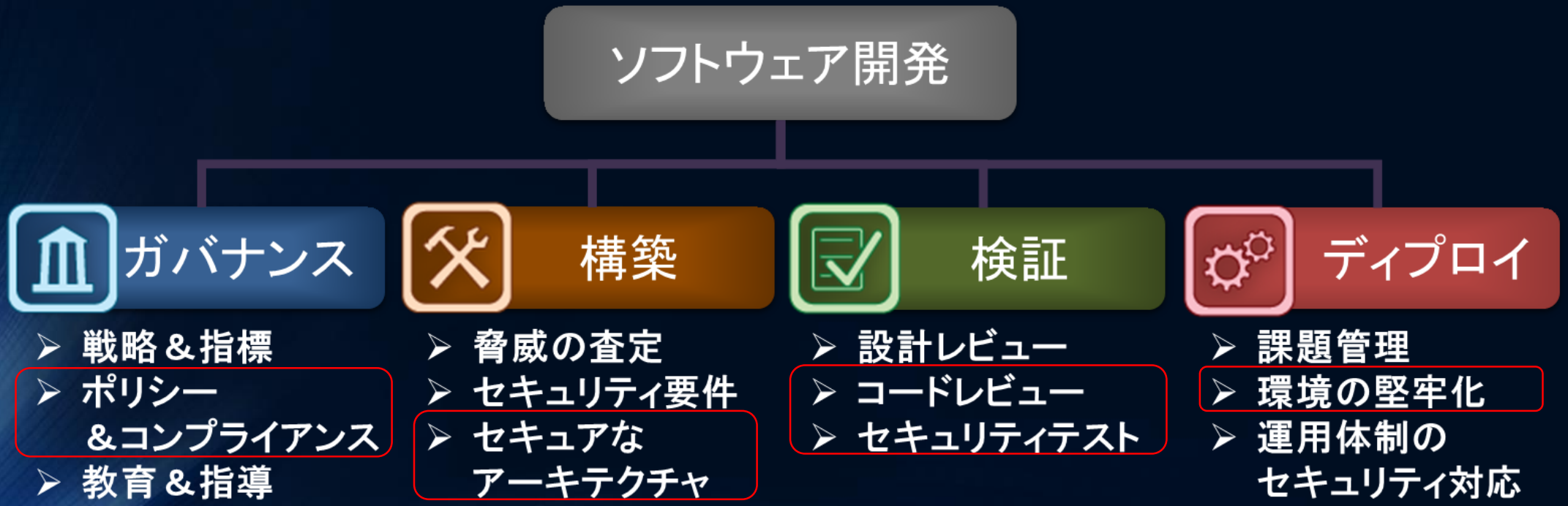
アプリケーションソフトウエアのセキュリティ向上に関する活動を展開する、フリーでオープンな世界規模のコミュニティ。

OWASPの使命は、一般利用者や組織がアプリケーションのセキュリティリスクについての意思決定を行う際に十分な判断材料が得られるように、アプリケーションのセキュリティを「可視化」すること。

OWASPには誰もが自由に参加でき、OWASPが作成する資料は、無償のオープンソフトウエアライセンスに基づいて公開される。OWASP Foundationは、米国国税庁（IRS）規定501条（c）項3号の認定を受けた非営利のボランティア組織としてOpenSAMM Projectの成果物を継続的に公開し、支援している。詳細については、OWASPのWebサイト（http://www.owasp.org）を参照のこと。

OpenSAMM

ソフトウェアセキュリティ保証成熟度モデルのカテゴリ



OpenSAMM V1.0を一部独自翻訳
https://www.owasp.org/images/a/a9/SAMM-1.0-ja_JP.pdf

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

～ コードレビュー ～

ソースコードのアセスメントを通じて、脆弱性を発見したり関連するリスク緩和活動を促すと共に、安全なコーディングに関する基本的な合意を形成していく

レベル	CR1	CR2	CR3
目的	出来る範囲で、コードレベルの脆弱性や高リスクなセキュリティ問題を検出する	コードレビューの精度と効率を自動化によって向上させる	総合的なコードレビューを行い言語レベルやアプリ固有のリスクを検出する
実施内容	A. セキュリティ要件からレビューチェックリストを作成 B. 高リスクのコードに対する部分的なレビューの実施	A. 自動コード分析ツールの活用 B. 開発ライフサイクルにコード分析を統合	A. アプリ特有の課題に対しコード分析をカスタマイズする B. コードレビューのためにリリース条件を確立

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

検証

～ セキュリティテスト ～

ソフトウェアのテストを通じて、脆弱性を発見するのはもちろんの事
ソフトウェアリリースにおける水準の合意を形成していく

レベル	ST1	ST2	ST3
目的	実装とソフトウェア要件に基づく基本的なセキュリティテストを実行する為のプロセスを確立する	開発中に行うセキュリティテストの完全性と効率が自動化によって向上する	ディプロイ前に基準となるセキュリティを確保する為、アプリケーション固有のセキュリティテストを要求する
実施内容	A. 既知のセキュリティ要件に基づいてテストケースを作成する B. ソフトウェアリリースに対する侵入テストを実施する	A. 自動セキュリティテストツールを利用する B. セキュリティテスト作業を開発プロセスに組み込む	A. アプリケーションに特化したセキュリティテスト自動化手法を採用する B. セキュリティテストを行う為のリリースゲートを設定する

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

～ ポリシー＆コンプライアンス ～

ガバナンス

組織全体のセキュリティ、コンプライアンス、監査を制御する枠組みを設定し、構築中および運用中のソフトウェアの保証を強化する

レベル	PC1	PC2	PC3
目的	ガバナンスとコンプライアンスについての当該組織に該当する推進要因を把握する	セキュリティとコンプライアンスの基本水準を設定し、プロジェクトごとのリスクを把握する	コンプライアンスを義務付け、組織全体のポリシーと標準に照らしてプロジェクトを測定する
実施内容	A. 外部のコンプライアンス推進要因を特定し監視する B. コンプライアンスの指針を設定し、維持管理する	A. セキュリティおよびコンプライアンスのポリシーと標準を策定する B. プロジェクト監査の方法を確立する	A. プロジェクトの為のコンプライアンスゲートを作成する B. 監査データ収集の方法を採択する

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

～ セキュアなアーキテクチャ ～

ソフトウェア構築時に、デフォルトで安全な設計（Secure-by-default）を実現する技術やフレームワークを採用する事を推進する

レベル	SA1	SA2	SA3
目的	事前予防的なセキュリティ指導について検討機会をソフトウェア設計プロセスに含める	既知のセキュアなサービスと「デフォルトでセキュアな設計」を採用する方向にソフトウェア設計プロセスを誘導する	ソフトウェア設計プロセスを公式に管理し、セキュアなコンポーネントの利用について認可制度を実施する
実施内容	A. 推奨ソフトウェアフレームワークのリストを維持管理する B. セキュリティに関する原則を設計に対して明示的に適用する	A. セキュリティに関するサービスやインフラを具体的に指定し、使用を奨励する B. セキュリティに関するデザインパターンをアーキテクチャに基づいて指定する	A. 公式なリファレンスアーキテクチャとリファレンスプラットフォームを確立する B. フレームワーク、パターン、プラットフォームの使用について認可制度を実施する

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

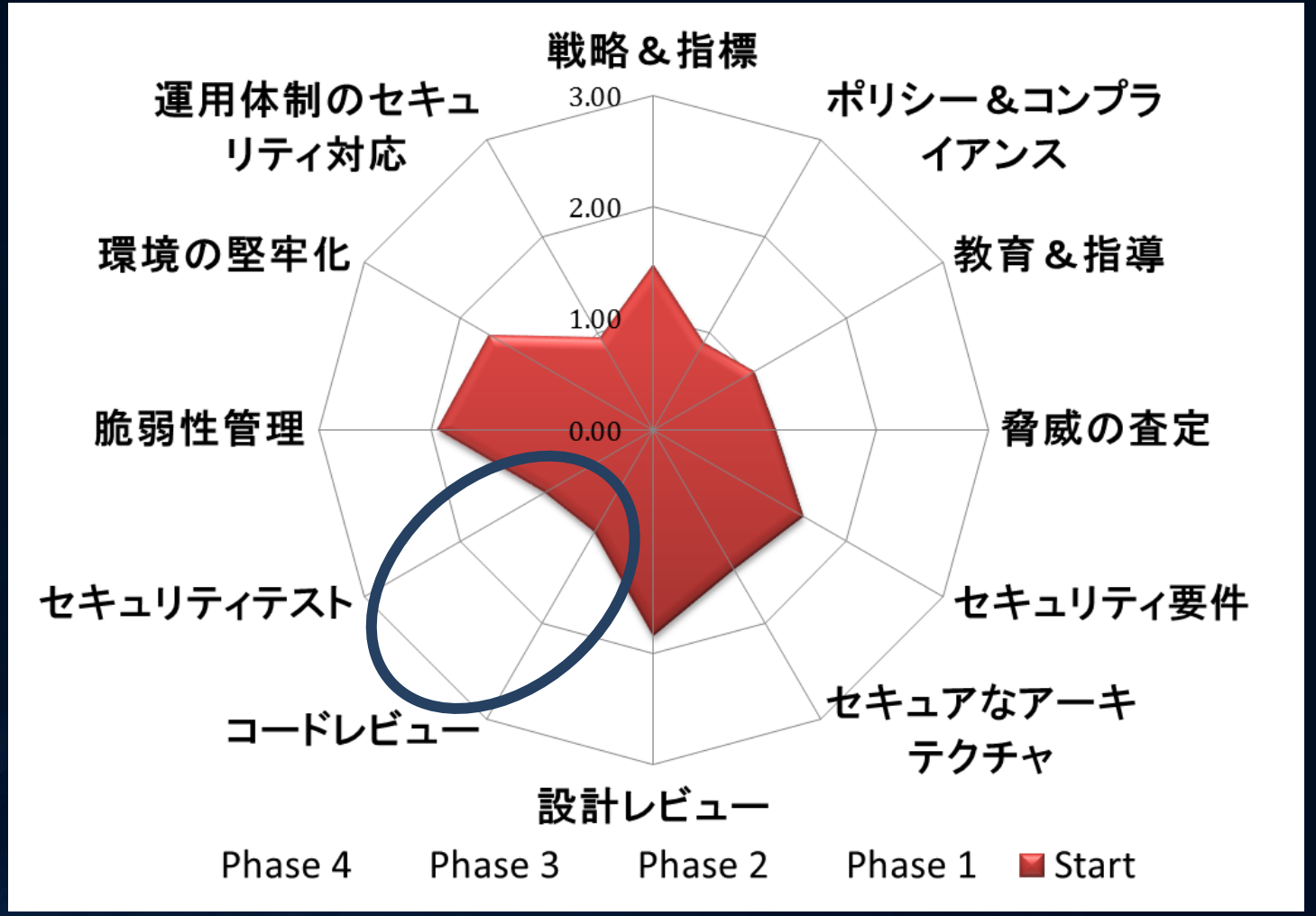
～ 環境の堅牢化 ～

ソフトウェアの運用環境に対して、適切なセキュリティ制御を実装し、ディプロイされるアプリケーションのセキュリティ保護体制を強化していく

レベル	EH1	EH2	EH3
目的	アプリケーションとソフトウェアコンポーネントに関する基準となる運用環境を理解する	運用環境の堅牢化によってアプリケーション運用の信頼度を向上させる	既知のベストプラクティスに照らしてアプリケーションの状況及び状態の妥当性を確認する
実施内容	A. 運用環境に関する仕様を維持管理する B. 重要なセキュリティアップグレード及びパッチを特定し、インストールする	A. 定期的なパッチ管理プロセスを確立する B. 基準となる環境構成の状態を監視する	A. 適切な運用保護ツールを指定し、ディプロイする B. 環境構成の監査プログラムを展開する

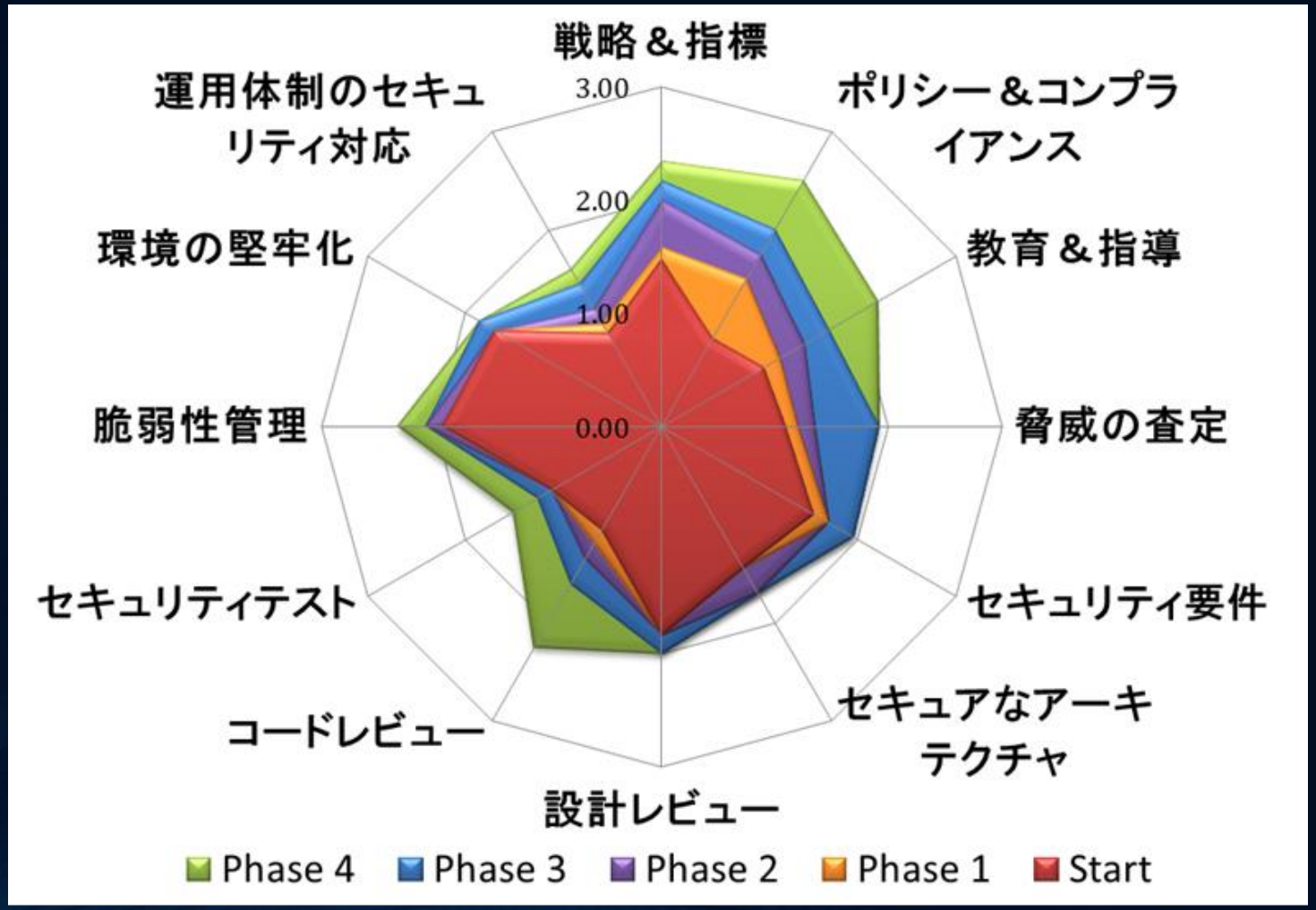
Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

現状の可視化



Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

セキュリティ対策のロードマップ作成



Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

① よりどころとなる指標を持つ ～ まとめ ～

AS IS

- OpenSAMMのような指標を使って現状を把握する

TO BE

- より上位のレベル実現に向けてロードマップを描く

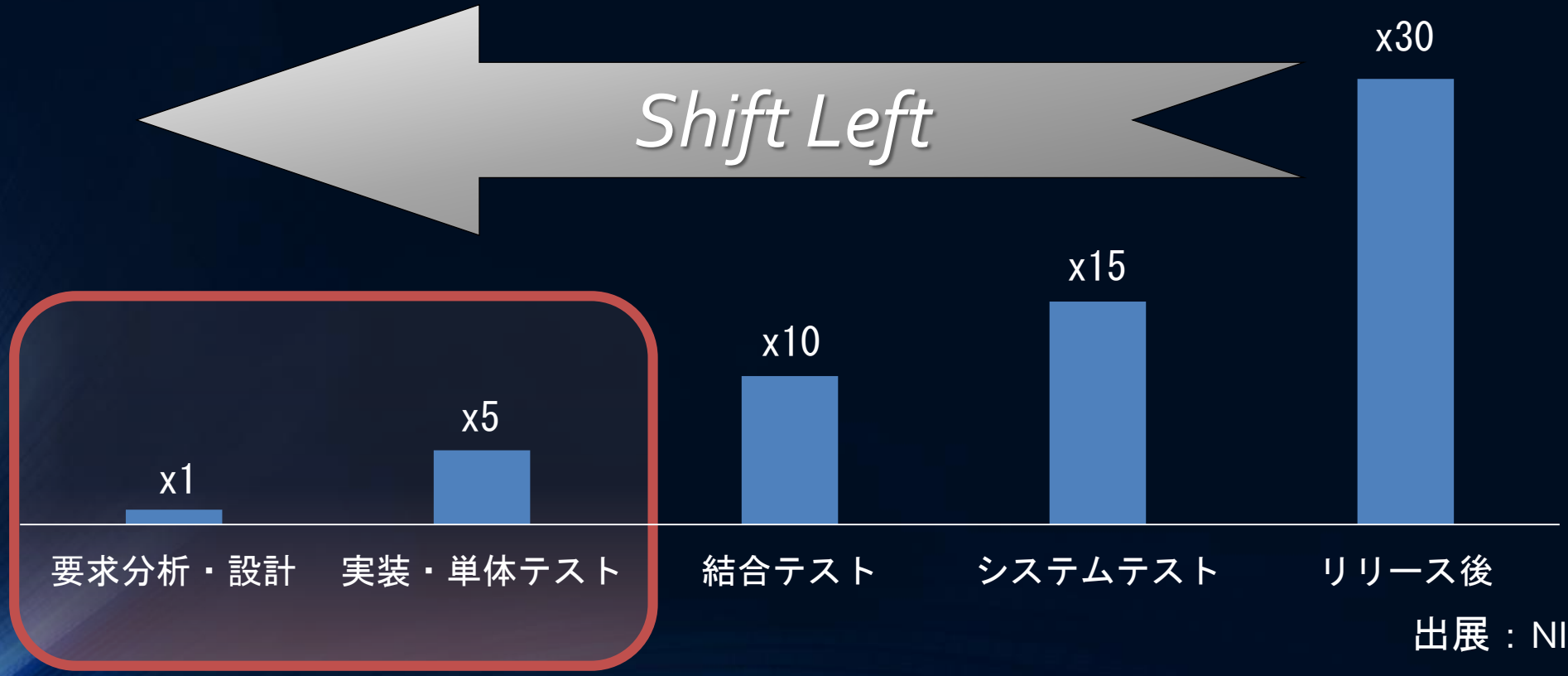
Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

② 具体的な活動を決める

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

セキュリティは開発ライフサイクル全体で対応

要求フェーズに見逃したエラーの修正コスト

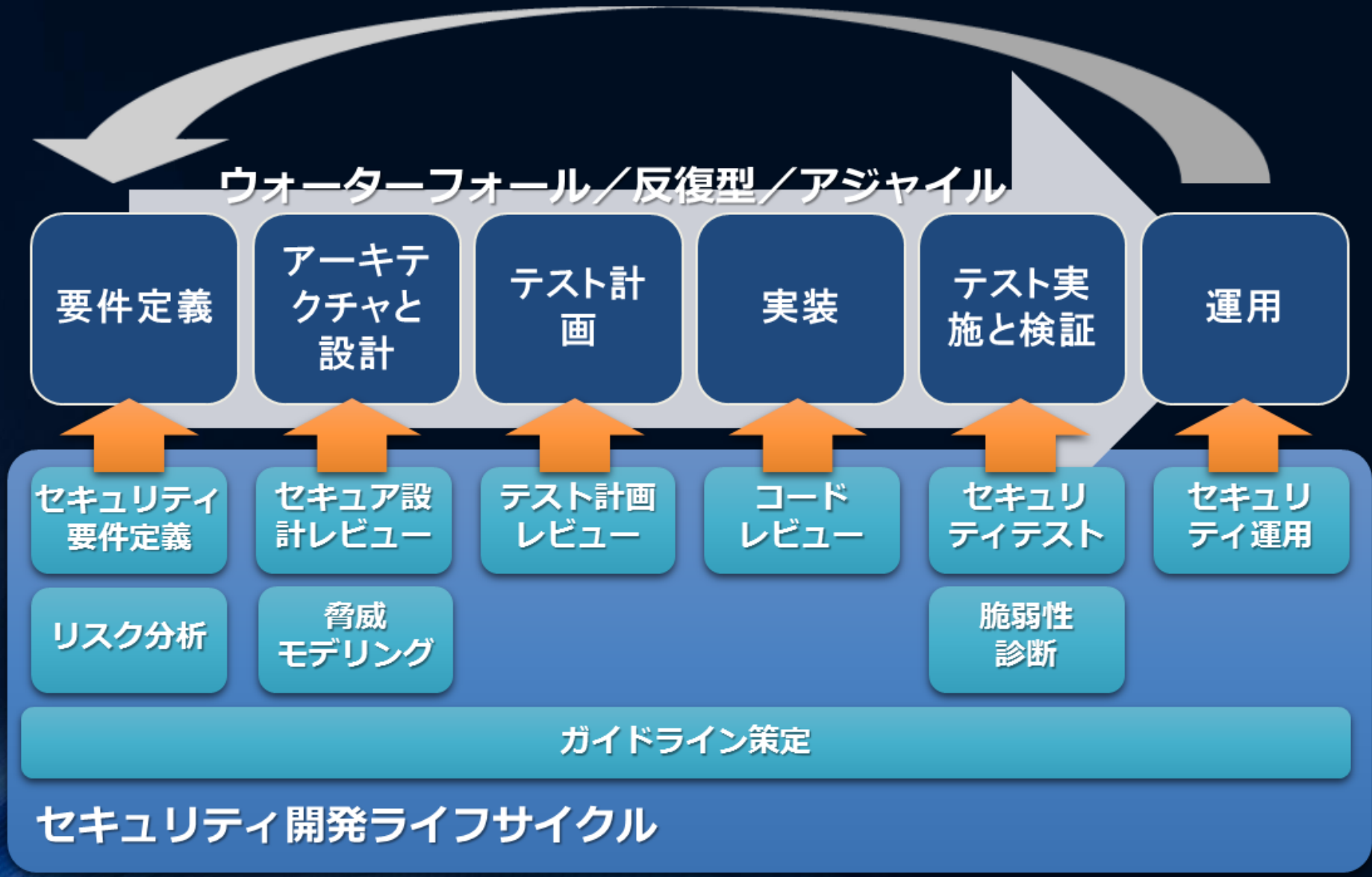


出展：NIST

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

開発ライフサイクル全体で対応するには？

セキュリティ開発ライフサイクルを実践する



Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

Example

要件定義フェーズでのセキュリティ対策

情報資産を守るためのセキュリティ要件を明らかにし、以降の設計・実装・テストにいたるまで、セキュリティ要件をベースに活動できるようにする

- 法律
- 規約
- ポリシー

- セキュリティ要件定義
- リスク分析

セキュリティ要件定義書

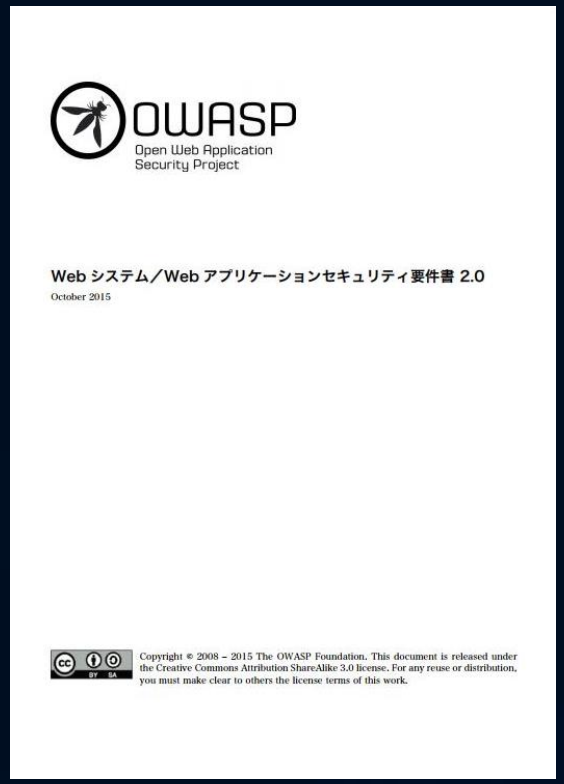
Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

セキュリティ要件定義 参考リソース

アプリケーションセキュリティ検証標準

https://www.jpcert.or.jp/securecoding/OWASP_ASVS_20160623.pdf

Webシステム／Webアプリケーション セキュリティ要件書 2.0



https://github.com/ueno1000/secreq

https://www.ipa.go.jp/security/vuln/websecurity.html

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

アーキテクチャと設計フェーズでのセキュリティ対策

より安全なフレームワークを選択したり、セキュリティ上の仕様バグを作りこまないようレビューする。また、設計上の脅威とリスクを整理する

- セキュリティ要件定義書
- アーキテクチャドキュメント

- セキュリティ設計レビュー
- 脅威モデリング

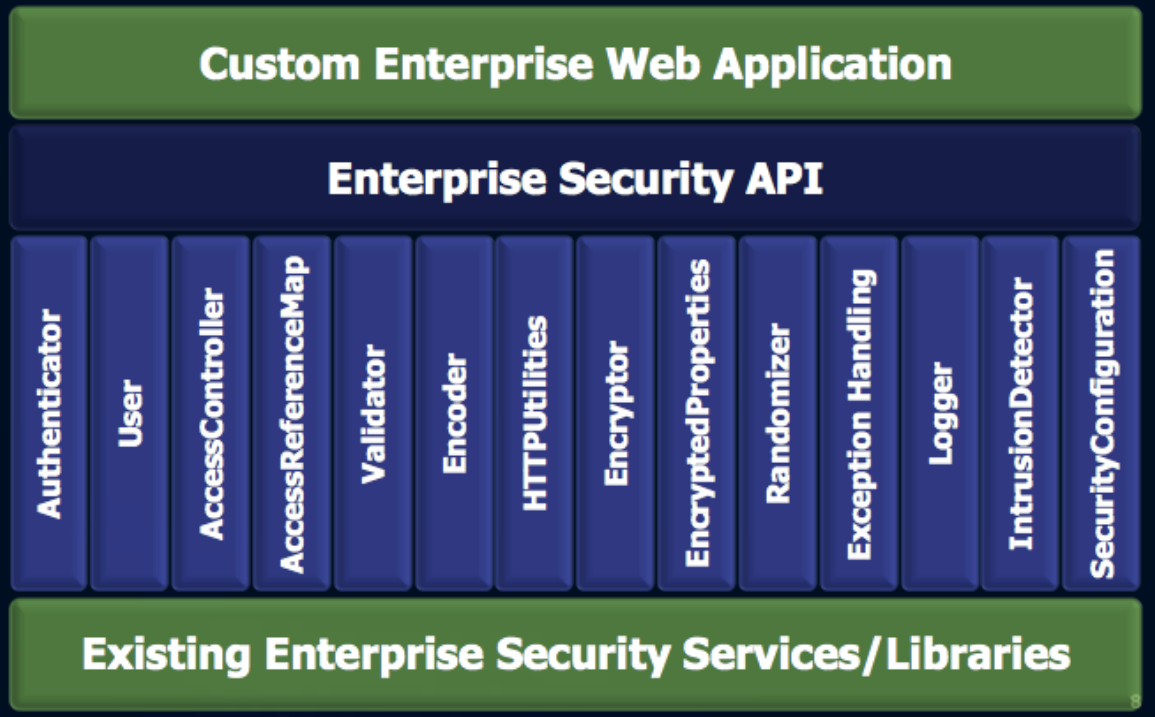
- セキュリティアーキテクチャ設計書
- 脅威とリスクの一覧

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

セキュリティ設計 参考リソース

https://www.ipa.go.jp/files/000052459.pdf

OWASP Enterprise Security API



https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=Home

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

Example

テスト計画フェーズでのセキュリティ対策

全ての脅威を取り除く事は出来ないので、受容するものも含め、
リスクを見積もりながら、テスト計画を策定する

脅威とリスクの一覧

- リスクベーステスト計画
- セキュリティテスト計画レビュー

- リスクベーステスト計画書
- セキュリティ制御一覧

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

Example

実装フェーズでのセキュリティ対策

セキュリティ開発規約などをベースに、セキュアなコーディングを行う
セキュリティ観点のコードレビューを行いより安全なコードを実現する

- セキュリティ開発規約
- セキュリティ制御一覧
- セキュリティアーキテクチャ設計書

セキュリティコードレビュー

セキュリティコードレビュー報告書

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

脆弱性対応 参考リソース

OWASP Top 10 – 2017が年内にリリース予定

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Proactive Controls

https://www.owasp.org/images/a/a8/OWASP_Top10ProactiveControls2016-Japanese.pdf

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

Example

テスト実施と検証フェーズでのセキュリティ対策

セキュリティ要件に基づいた、セキュリティテストを行ったり、
脆弱性診断などを行い、リリース前の確認を行う

リスクベース
テスト計画書

- セキュリティテスト
- 脆弱性診断

- セキュリティテスト報告書
- 脆弱性診断報告書

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

Example

運用フェーズでのセキュリティ対策

逐次更新される脆弱性に関する報告を元に、パッチの適用を検討したりインシデントの分析結果を前段の適切な開発フェーズにフィードバックして改善する

- セキュリティ要件
- パッチ適用ポリシー
- 変更管理ポリシー

- セキュリティ運用
- 運用状況レビュー

- インシデント等セキュリティレビュー報告書
- 更新済みセキュリティ関連ドキュメント

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

② 具体的な活動を決める ～ まとめ ～

- 自社の開発プロセスに沿った、セキュリティ活動を選択し統合する

③ すみずみまで何度も繰り返す

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

アプリケーションレイヤーのセキュリティ関連ツール

SAST (Static Application Security Testing)

- 静的テスト、ホワイトボックステスト

DAST (Dynamic Application Security Testing)

- 動的テスト、ブラックボックステスト

IAST (Interactive Application Security Testing)

- DAST と SAST の組合せ
- テストを実行するエージェントとして実装される

RASP (Runtime Application Self-Protection)

- リアルタイムに脅威を特定、ブロックする仕組み。ガートナーが提唱

SCA (Software Composition Analysis)

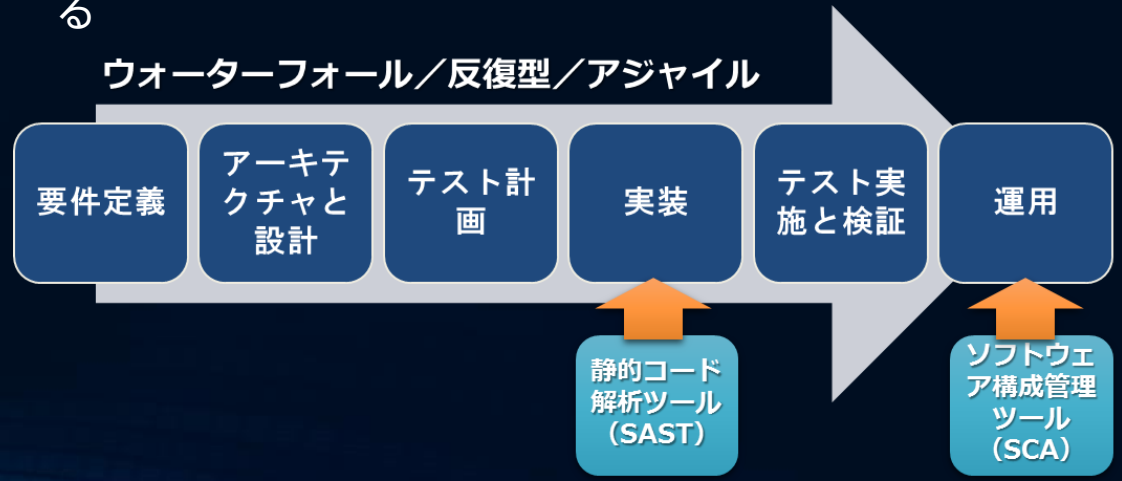
- ソフトウェアを構成するOSSやサードパーティ製のコンポーネントを解析する

モバイルアプリの振舞い解析

- モバイルアプリの危険な振舞いを検知する

ペネトレーションテスト

- 攻撃者と同様の手口で攻撃することで脆弱性を検出する

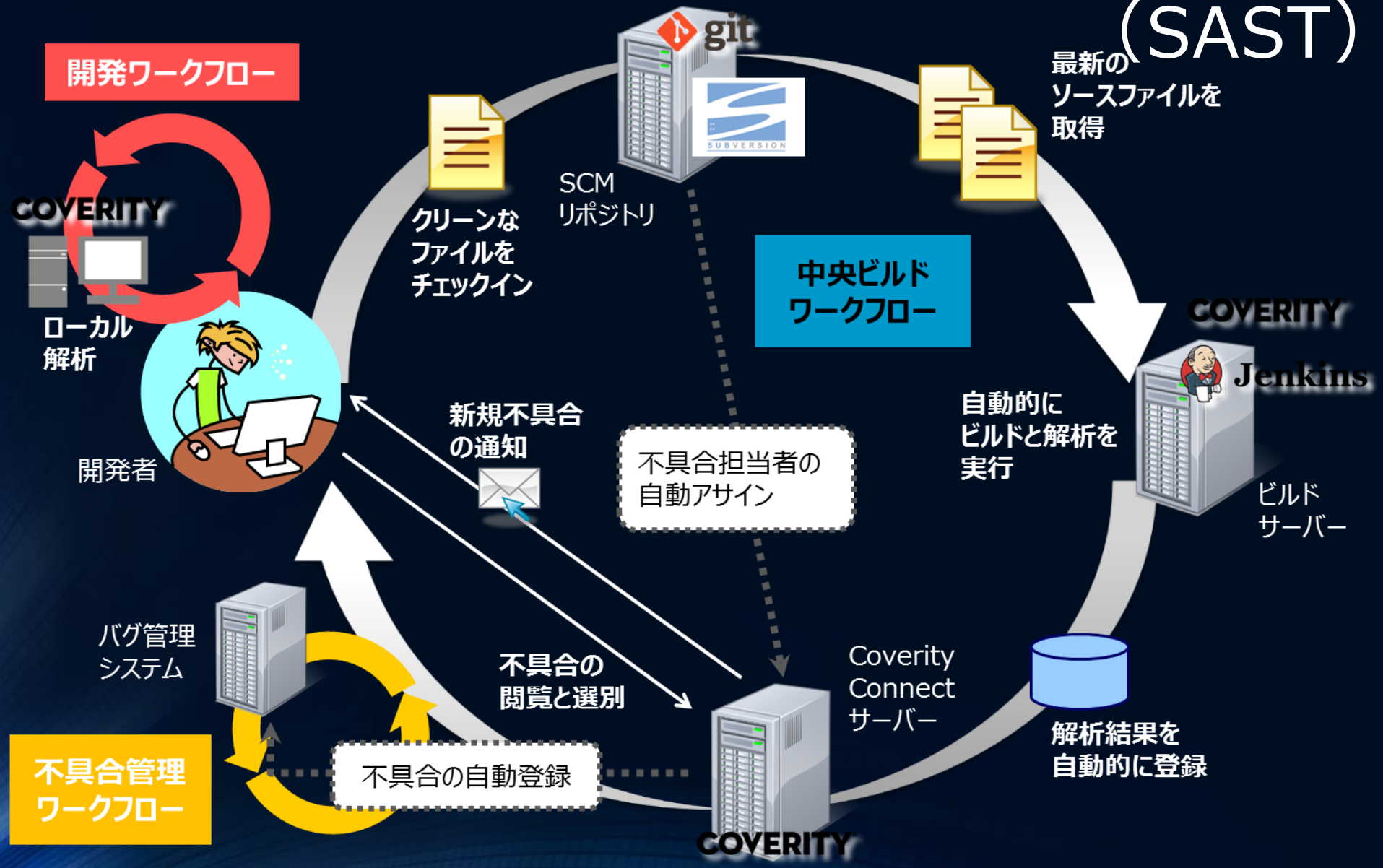


Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

開発プロセスに組み込まれたコードレビューツール（SAST）

検証

CR2



Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

静的コード解析ツール（SAST）適用の実施例

ある開発案件で当初より静的解析ツールCovertityを利用した結果、
プログラムの問題発見・修正の生産性が向上

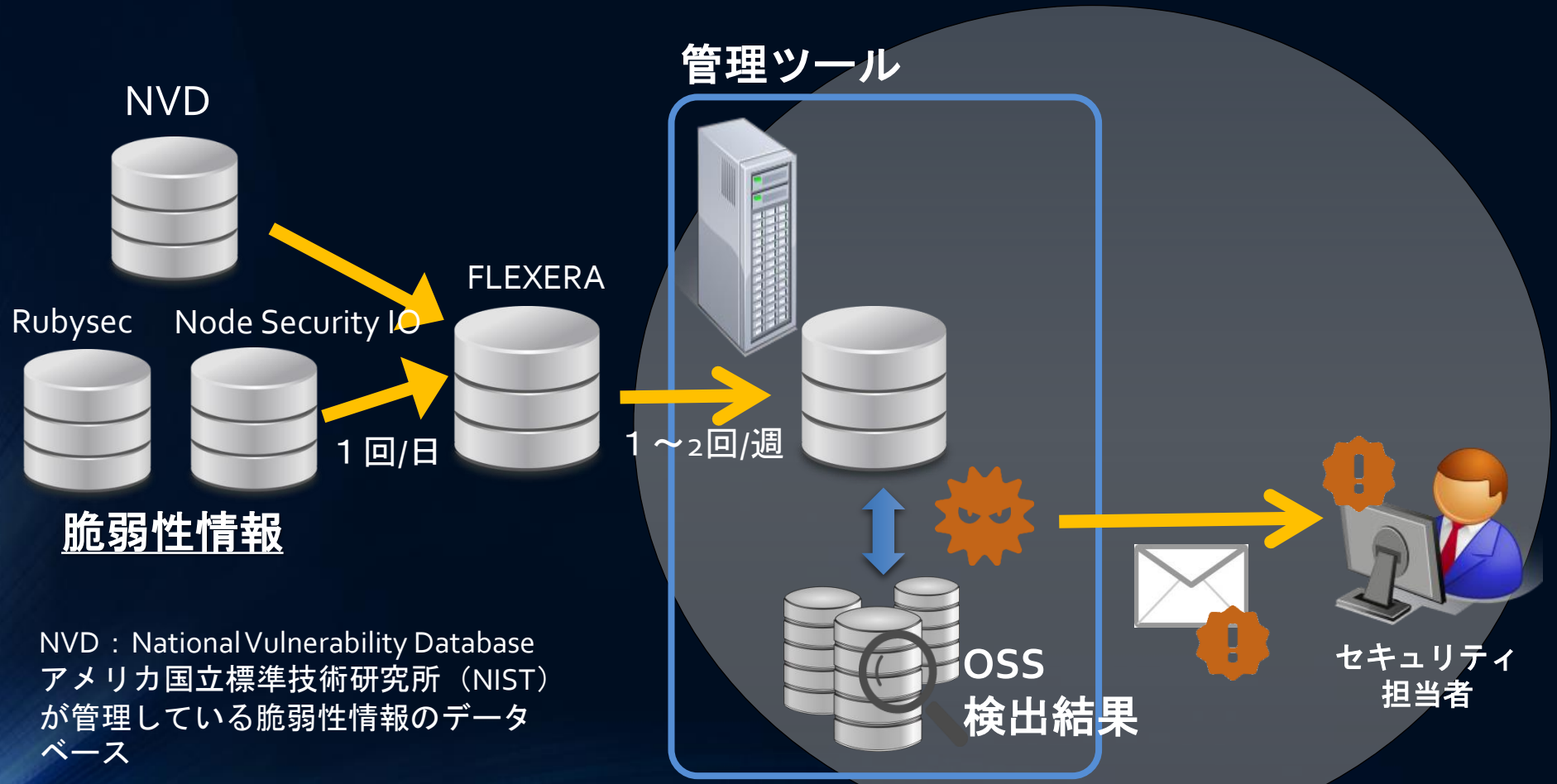
約2800時間＝17.5人月の工数削減効果と品質改善効果

- 定量効果
  - **費用対効果：2800時間**
    - 約36万行のコードに対して、問題発見件数：239件、問題修正件数：200件
    - 一件当たり14時間の工数削減効果
- 定性効果（品質改善）
  - **通常のレビュー・テストでは発見しにくい不具合**を**早期に検出**できた

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

OSS利用におけるライセンス管理/脆弱性管理に関するツール活用

EH2



NVD：National Vulnerability Database
アメリカ国立標準技術研究所（NIST）が管理している脆弱性情報のデータベース

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

SA1

OOS管理ツールを用いた OSS利用に関するポリシー設定とワークフロー

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

③ すみずみまで何度も繰り返す ～ まとめ ～

- 人手では質・量とも不可能なレベルの作業を自動化ツールを用いて何度も行いセキュリティ保証のレベルを上げる

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

まとめ
～ ３つのポイント ～

① よりどころとなる指標を持つ
⇒ OpenSAMMを利用してロードマップを描く

② 具体的な活動を決める
⇒ セキュリティ開発プロセスを作成し実践する

③ すみずみまで何度も繰り返す
⇒ 自動化出来るところはツールを活用する

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

ご清聴ありがとうございました

【お問い合わせ先】
株式会社オージス総研
TEL: 03-6712-1201
mail: info@ogis-ri.co.jp

アプリケーションセキュリティソリューション
http://www.ogis-ri.co.jp/product/1264816_6798.html

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

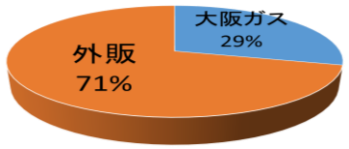
【参考資料】

会社紹介

株式会社オージス総研

- 代表者：　代表取締役社長　西岡　信也
- 設　立：　1983年6月29日
- 資本金：　4.４億円　（大阪ガス株式会社100%出資）
- 事業内容：　システム開発、プラットフォームサービス、コンピュータ機器・ソフトウェアの販売、コンサルティング、研修・トレーニング

- 主な事業所
  - 本　社：　大阪府 大阪市西区千代崎3-南2-37 ICCビル
  - 東京本社：　東京都 港区港南2-15-1 品川インターシティA棟
  - 千里オフィス：　大阪府 豊中市新千里西町１－２－１
  - 名古屋オフィス：　愛知県 名古屋市中区錦1-17-13 名興ビル
- 売上実績：　642.8億円（連結）　371.3億円（単体）　(2016年度)
- 従業員数：　3,284名（連結）　1,407名（単体）
- 関連会社：　さくら情報システム（株）、（株）宇部情報システム、（株）システムアンサー、OGIS International, Inc. 、上海欧計斯軟件有限公司（中国）
- オージス総研グループ 売上構成比（連結）



取得許可認定

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料

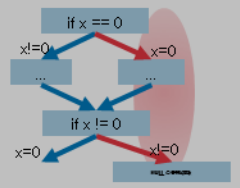
静的コード解析ツール「Coverity」

開発段階でバグや脆弱性を発見できれば、テスト工程やリリース後の手戻りを減らすことができるだけでなく、動的なテストでの発見が容易ではないレア・ケースの不具合に早期に対処ができます。Coverityは独自のフロー解析・統計解析アルゴリズムによりソースコードを検査し、誤検知率15%以下という高精度でバグや脆弱性を検出します。

トップクラスの高精度を支える独自アルゴリズム

SATソルバ

不具合が発生しないパスを排除し、誤検知を減らす



全パス&関数間解析

関数またはファイルに跨る不具合の検出

統計的な解析

プログラムの目的を推測し、予期しない動作を報告

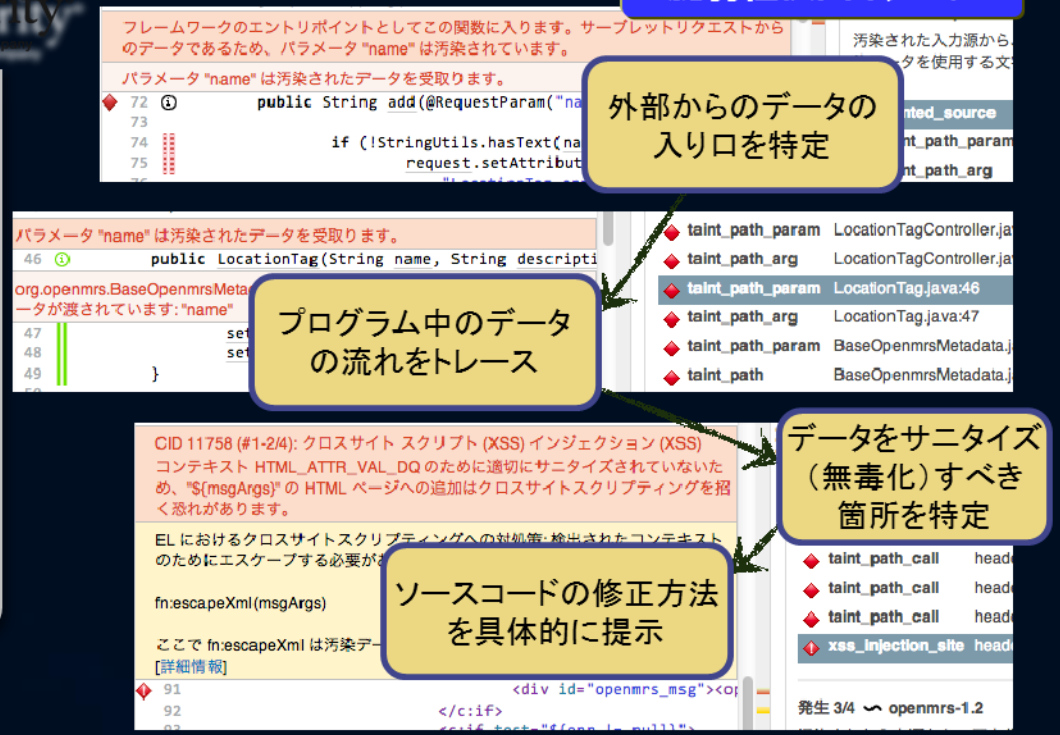
```
int *p = malloc(sizeof(int));
if(p != 0)  *p = 42;
...
int *p = malloc(sizeof(int));
if(p != 0)  *p = 42;
```

多分正しい

```
int *p =
    malloc(sizeof
    (int));
*p = 42;
```

多分間違い

脆弱性検出イメージ



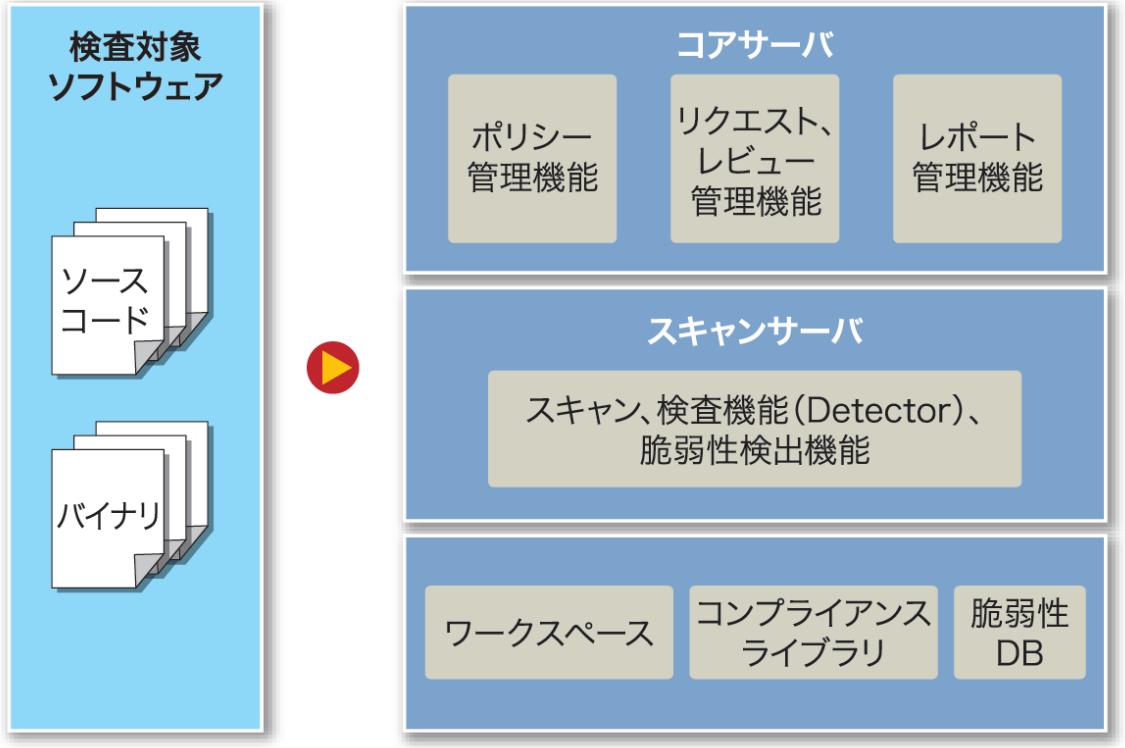
高精度でソースコード中の不具合・脆弱性を検出します

開発チームの各SEに対し、デイリーで各人が作りこんだ不具合・脆弱性を通知することで、開発しながらこれらの問題を修正。良好な品質状態でテストやセキュリティ診断工程に進むことを可能にします。

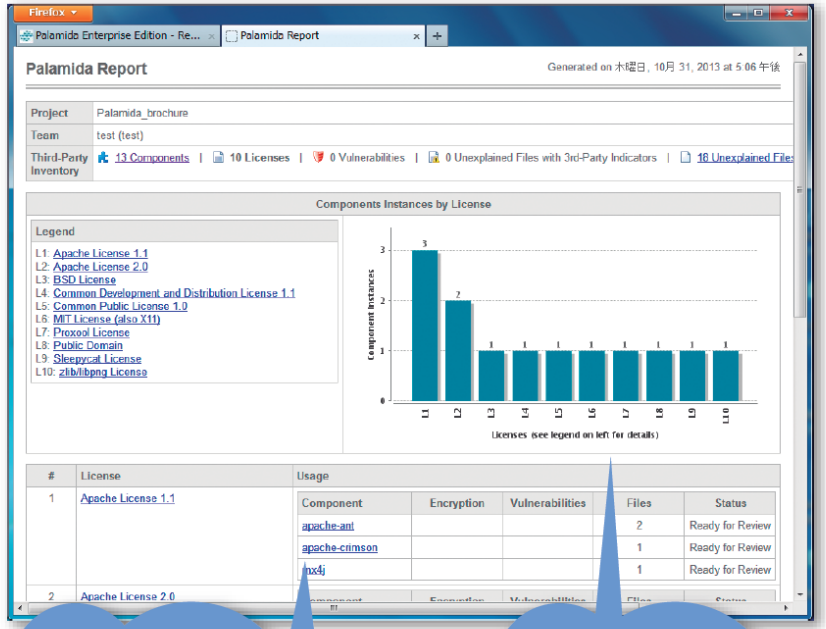
※CoverityはSynopsys, Inc.の米国およびその他の国における商標または登録商標です。

オープンソースソフトウェアのライセンス・脆弱性管理ソフト「Palamida」

機能概要



検査レポート（OSS成分表）



ライセンスごとに
分類されたOSSのリスト

検出されたライセンスの
リストと種類の比率

Copyright © 2017 OGIS-RI Co., Ltd. 2017/9/28「システム開発におけるアプリケーションセキュリティ３つのポイント」講演資料