SOMPO ホールディングス | 保険の先へ、挑む。

【事例紹介】
損保ジャパンにおけるOSS利活用及び管理手法について

-経済産業省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース向け-

2021.1.13

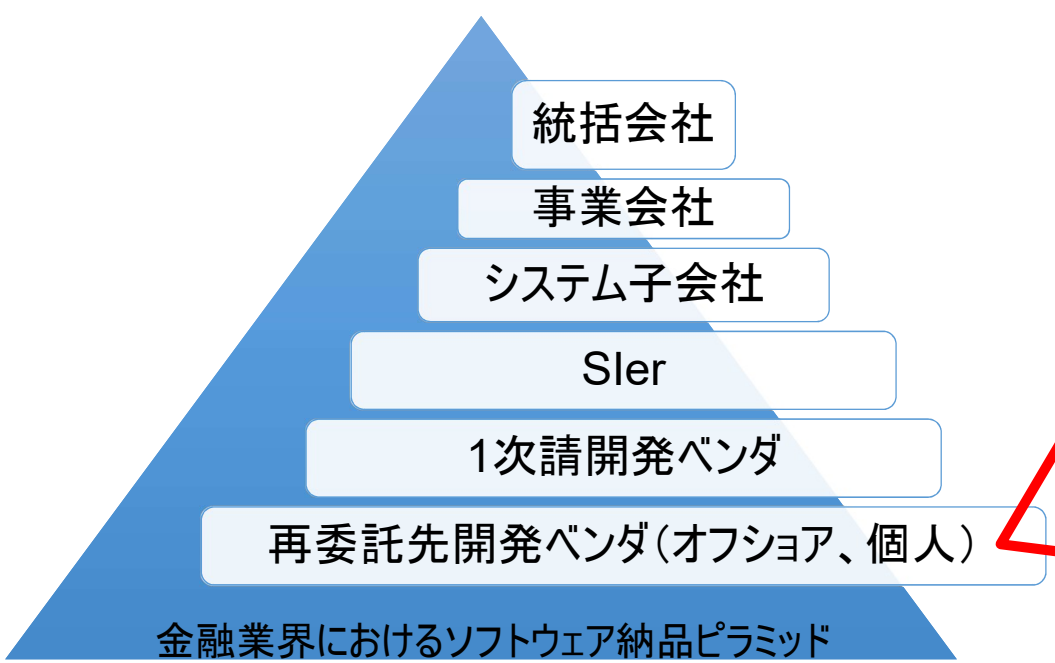
損害保険ジャパン(株)

IT企画部

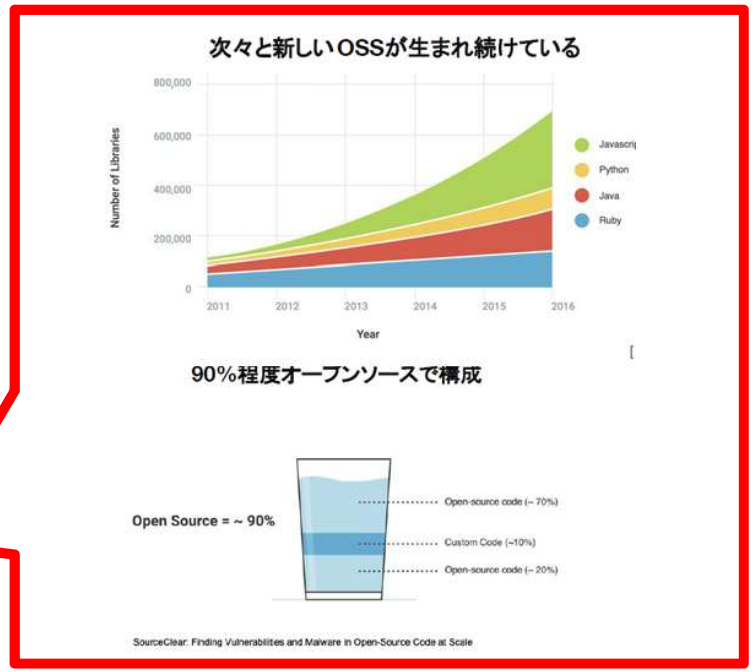
セキュリティエバンジェリスト　小中　俊典

はじめに　～金融システム・サービスにおけるOSS利用の状況～

- 日本の金融機関における一般的なシステム・サービス開発では、システム子会社を利用した多段開発納品スタイルが未だ主流である。一方、実開発現場ではオフショア、ニアショア、個人事業主などある程度フリーなスタイルでの開発がおこなわれ、開発者はOSSを積極的に利用し生産性を高めている。
- 事業会社やシステム子会社にはSIer以下の委託先がどのようなOSSを利用し、業務システム・サービスを開発されたのかがわからず、SIerとの保守契約のみで維持運用を行っている状況が多く見受けられる。もちろん、事業会社側としてもITIL準拠にて構成管理や資産管理等を行っているがそれではOSS管理レベルとしては不十分と考えている。

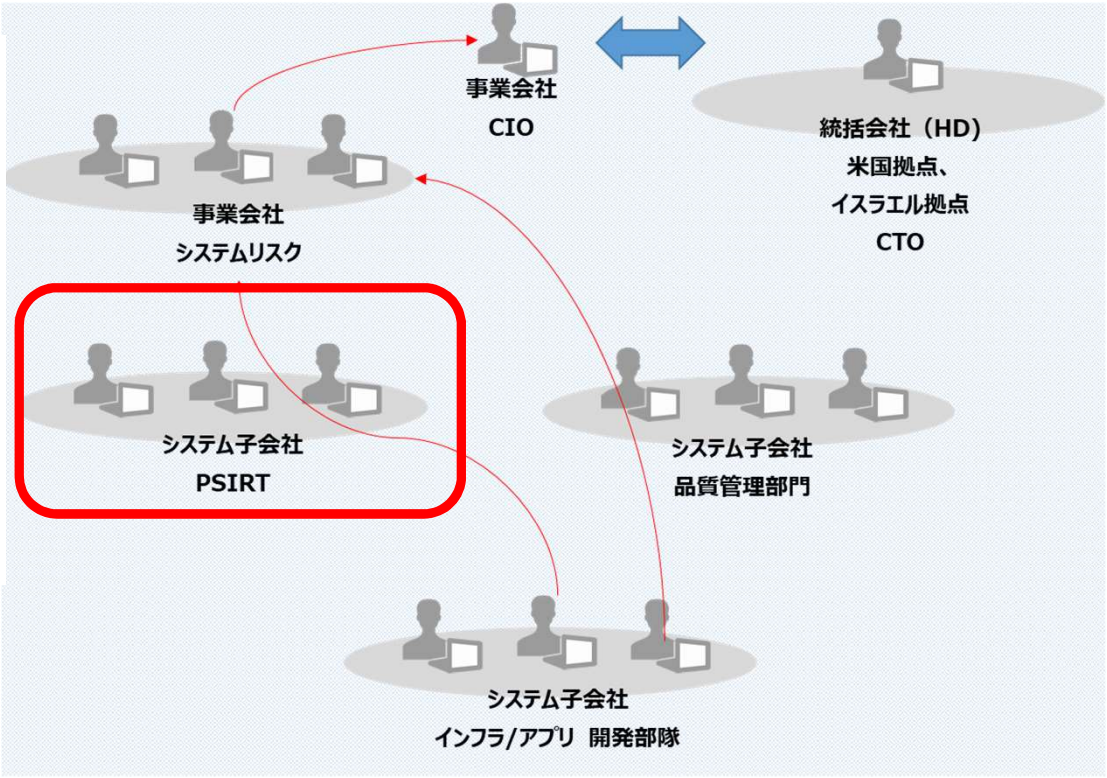


金融業界におけるソフトウェア納品ピラミッド



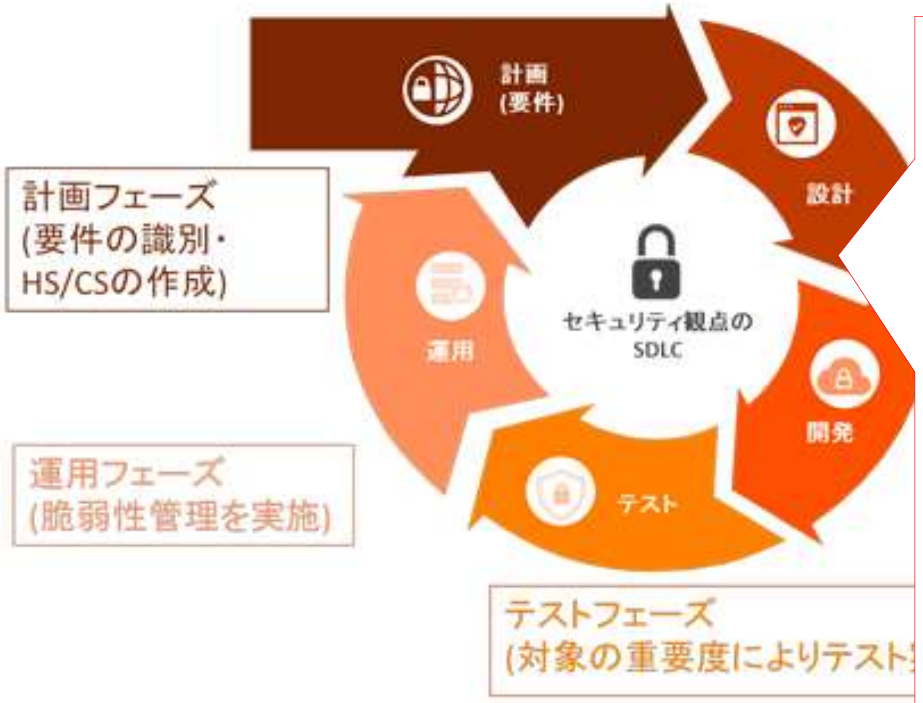
【概要】当社におけるOSS利活用に向けたセキュリティ対策

- 当社はソフトウェア開発ライフサイクル（SDLC）におけるセキュリティ対策としてOSSならびにSoftware Bill of Material：ソフトウェア部品表（以下、SBOM）を管理している。
- SBOMは脆弱性管理やリスク管理で利用するため、品質管理部門とは独立したProduct Security Incident Response Team（以下、PSIRT）に準ずる専任組織にて利用実態を把握、管理し、事業会社のシステムリスク部門と連携し、リスク低減を行っている。



【概要】当社におけるOSS利活用に向けたセキュリティ対策

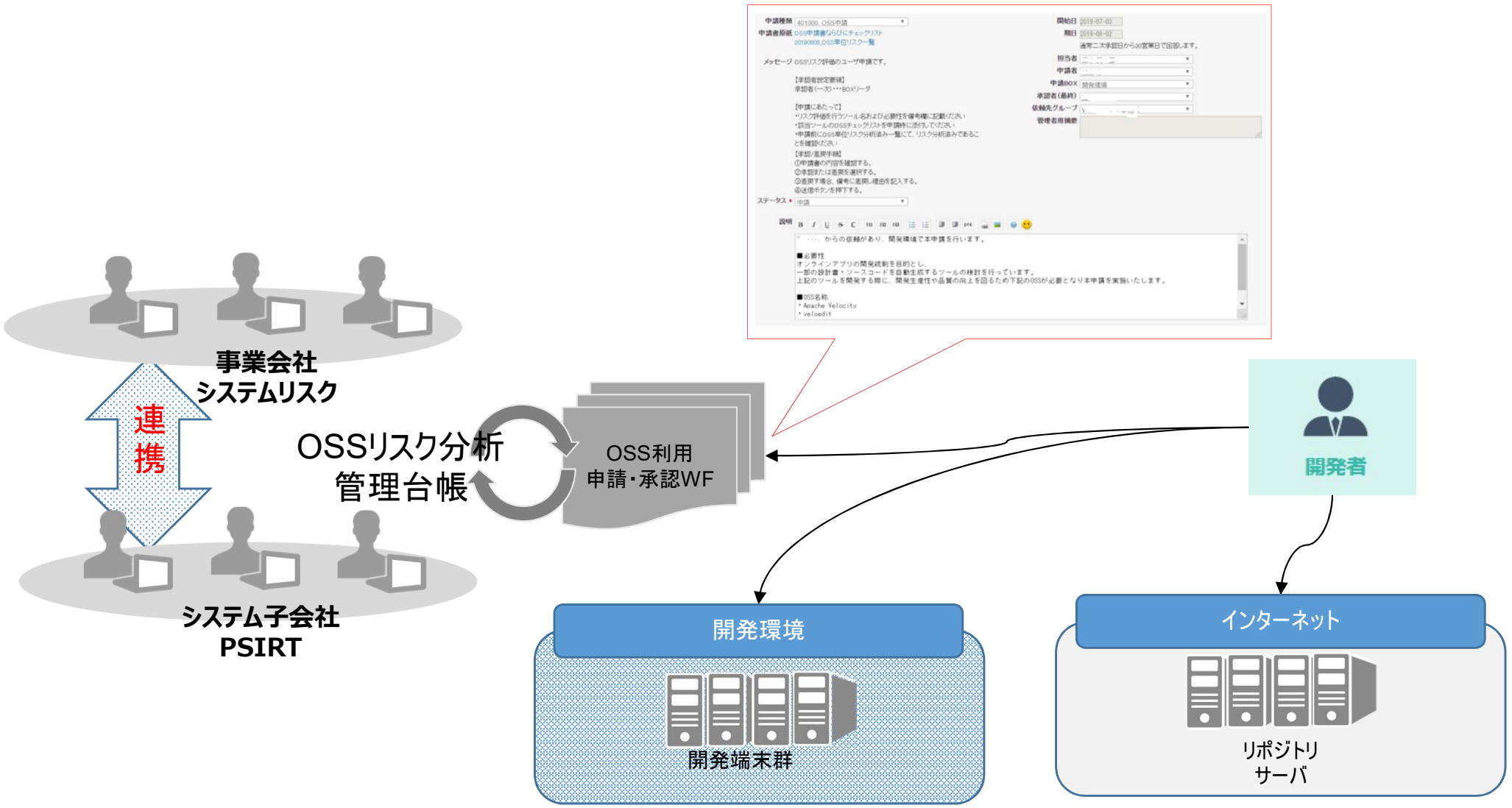
- 当社ではSDLC内でOSSならびにSBOMの妥当性確認を開発前、開発中、開発後の3フェーズで作成、管理、チェックを行っている。



- 【開発前：計画・設計】申請ベースでの確認方法
  社内のレビュー体制活用
  ⇒調達管理への組み込み
- 【開発中：開発・テスト】実機ベースでの確認方法
  ミドルウェア、ソフトウェアの解析自動化の仕組み
  ⇒開発工程管理への組み込み
- 【開発後：運用】リスト化と運用方法
  構成情報の抽出、登録管理
  ⇒構成管理、脆弱性管理、リスク管理への組み込み

【開発前】当社におけるOSS利活用に向けたセキュリティ対策

- 開発着手前の時点で開発者が利用したいOSSを大枠で把握し、管理するために以下、申請・承認のWFにて、OSS利用情報収集、リスク分析、管理を行っている。



【開発前】当社におけるOSS利活用に向けたセキュリティ対策

- OSSリスク分析としては、以下の15項目を対象として、調達管理へ組み込み、大枠でOSS利用の妥当性を確認している。

NO	リスク分類	リスク又は注意点
1	提供元の調査【確認事項】	OSSは自然消滅、開発停滞など、安定性や持続性といった面でのリスクがある
2	情報量及び質【確認事項】	使用方法等の情報量が少ない場合や情報の質が低い場合、工数増につながる可能性がある
3	品質【確認事項】	OSSは品質保証がなく、自己責任での活用が前提
4	保守性【確認事項】	OSSはソースコードが公開されているが、それを理解し不良対策を行うことは困難な場合がある
5	活用形態【対応事項】	活用形態によりライセンス上の義務、知的財産権上のリスクが異なる
6	遵守【対応事項】	条件の不遵守によりライセンス違反が生じる
7	ライセンスの特定【対応事項】	適用ライセンスの確認が不十分、不正確なことによりライセンス違反が生じる
8	ライセンスの選択【対応事項】	適用ライセンスを選択可能なOSSについてはリスクの低いものを選択
9	コピーレフト型OSS活用時のリスクへの対応【対応事項】	ライセンス互換性確認漏れによる、ライセンス違反およびOSSの継続利用不可
10	特許の確認【確認事項】	OSSに含まれている第三者の知的財産の侵害
11	輸出管理【確認事項】	OSS部分の輸出関連法規違反
12	評価【確認事項】	OSSと製品等の仕様との整合性，利用環境との整合性の確認漏れによる問題発生
13	外注契約【対応事項】	外注先が独自判断もしくは意図せずOSSを利用してしまう
14	納品【対応事項】	ライセンス義務の履行
15	保守【確認事項】	保守対応遅れ、その他問題発生

分析結果例

OSS名	概要	システム・サーバ(重複利用時のみバージョンを記載)								リスク分類			
		開発FW	プロ管ツール	Lib管理 構成管理サーバ	Lib管理 リリース管	開発インフラ CI/静的解	開発インフラ ビルド/リポジト	端末ソフトウェア	FW	利用バージョ	品質(脆弱性)	輸出管理	ライセンス義務の発
PostgreSQL	オブジェクト関係データベース管理システム	○(9.4.5)									※2		
					○(9.5.3)						※2		
						○(9.4.5)					※2		
Redmine	Webベースのプロジェクト管理ソフトウェア。 タスク管理、進捗管理、情報共有が行える。		○										
MySQL	関係データベース管理システム（RDBMS）の一つ。		○								※2		

【開発前】SBOMの手動収集・管理の課題

- 当初、当社において、開発前のOSSリスク分析のみで十分と判断していたものの、開発が進むにつれ、以下のような課題が判明した。

✓開発者によるOSS利用申請では申請内容にバラつきが出て粒度に問題がある。また、OSS内部で利用しているOSSライブラリ情報まで記載できない。（下表）

✓脆弱性情報と突合処理すると、フォールスポジティブ、ネガティブが多く発生。

✓手動のため情報更新頻度が年ごとになり鮮度が古く、日々更新される更新されるOSS（ライブラリ含む）、脆弱性情報に追従できない。

✓開発前、開発中で開発端末にリポジトリサーバからOSS（ライブラリ含む）を自動ダウンロードする可能性があるため、PSIRTが知らない間に脆弱性が混入。

JDK
GlassFish
JavaHL
Subversion
PostgreSQL
Redmine
MySQL
Ruby
・・・・・・・・

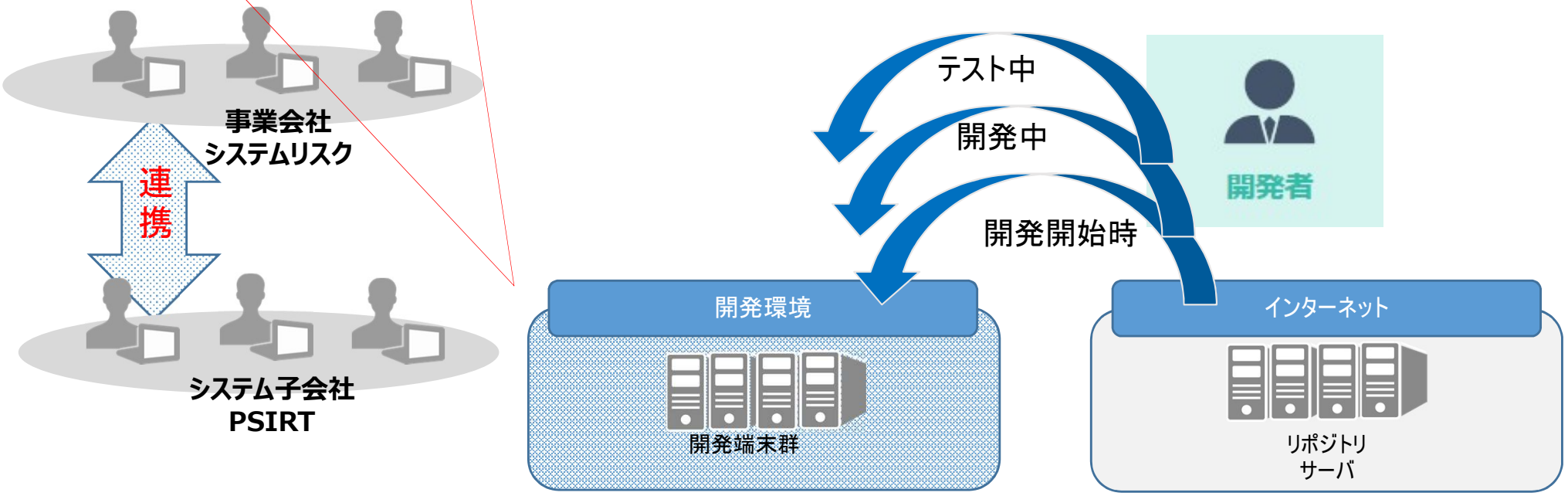
対策

SBOMの作成と管理の自動化をSDLCへ組み込み

【開発中】当社におけるOSS利活用に向けたセキュリティ対策

- 開発中は開発者が実装で利用するOSSが申請通りでは無いことがある。開発者は開発中、テスト中において必要に応じOSSを取り込む必要性がある。そのため開発中においても定期的にSBOMを作成し、管理していくことが望ましいと考えている。

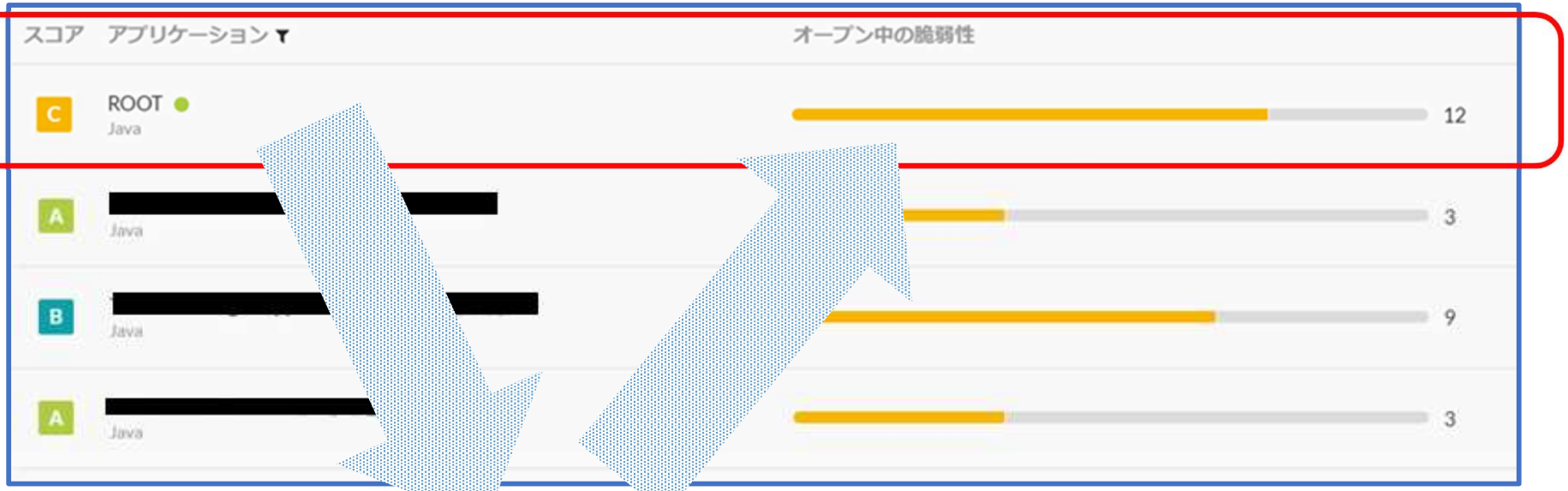
✓申請時にもれたOSS検出
✓詳細レベルでのOSS検出
✓システム・サービス動作上のOSS利用実態把握
✓開発環境に持ち込んだ全OSSの危険性把握



【開発中】当社におけるOSS利活用に向けたセキュリティ対策

- 当社におけるSBOM自動収集・管理の事例

  自動でSBOMを作成・管理するツール導入
  アプリ単位でSBOMを管理し、危険度と脆弱性数を表示



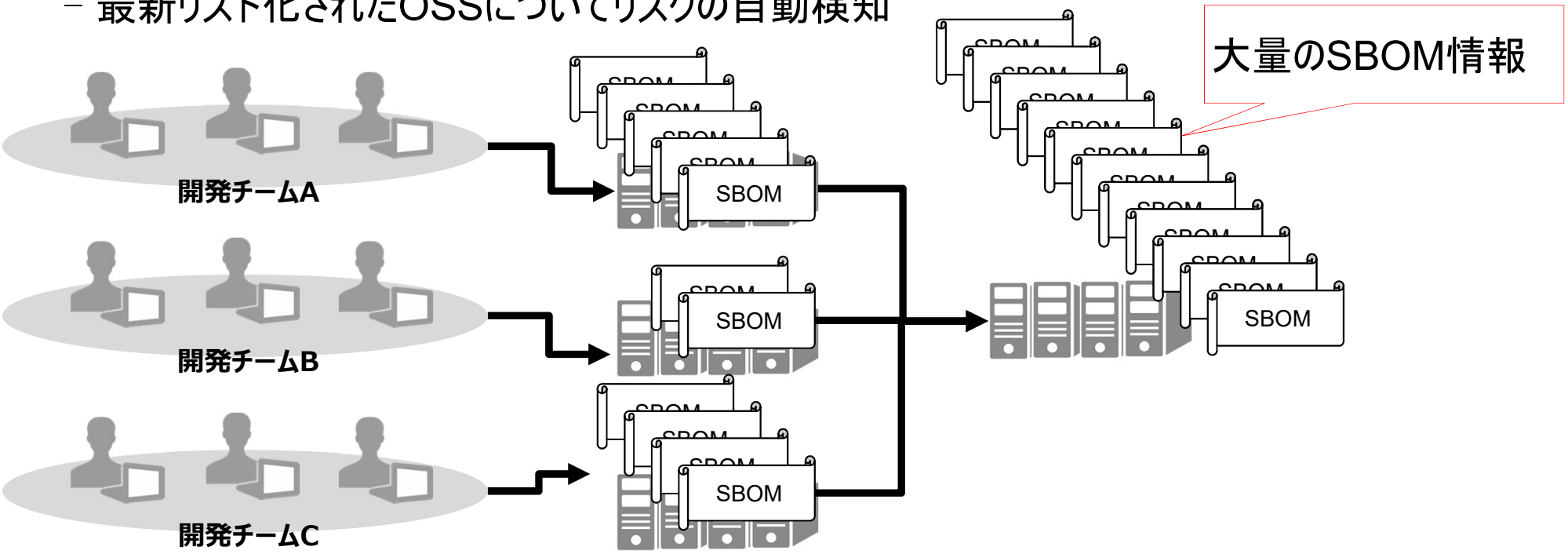
作成したSBOMはツリー形式で管理
日次でSBOMを作成し、脆弱情報とマッチング処理を実施

補足：SBOMの管理粒度

- SBOMは作成納品されたソフトウェアのリスク評価に利用するため、脆弱性情報に合わせた粒度での作成が必要になる。以下の例では1つのOSS（Spring-web5.2.11）に対する依存構造を示しており、最下層の部品名とバージョンまでを管理する必要がある。

【開発後】当社におけるOSS利活用に向けたセキュリティ対策

- 開発後のリリース・運用においても、開発中に作成されたSBOMを継続管理する必要がある。理由としては、不定期でのOSSバージョンアップ/変更（機能、サポート、脆弱性、開発停止等）が発生するためである。これに対応するため、SBOMを利用した脆弱性・リスク管理を行い自社システム・サービスにOSSバージョンアップ必要か否かを即時に検知する必要がある。また、開発者やセキュリティ管理者等との連携が必要となるためコミュニケーションツールやPJ管理などと連携していることが望ましい。
  - 自社サービス全体でのOSS利用状況を管理
  - 自社サービス全体での利用OSS全量を最新リスト化
  - 最新リスト化されたOSSについてリスクの自動検知



補足：ツール連携

- 日々脆弱性情報と照合し、新たな脆弱性が発見されたらセキュリティ担当・管理者・開発者へメール通知され、PJ管理ツールへも連携。

例

【まとめ】全体像

- 従来から行っている開発前の開発者申請ベースでのOSSリスク低減・回避策は維持。
- 開発中以降は自動的にSBOMを作成し、開発効率を維持したままリスク低減・回避を実現。
- 大規模なシステムやサービスになればなるほどSBOM管理は複雑化するため、自動化された仕組みでの継続運用が必須。
- OSS利用は開発効率を上げるために必要不可欠なものであり、利用禁止は困難。開発現場において、開発効率を阻害しないようリスク低減・回避を行う必要がある。