OSS管理＆SBOM管理ツール
Black Duck

株式会社 日立ソリューションズ

OSS活用に伴うリスクに対応できていますか？

セキュリティリスク

OSSの脆弱性を突いたハッキング・情報漏洩

コンプライアンスリスク

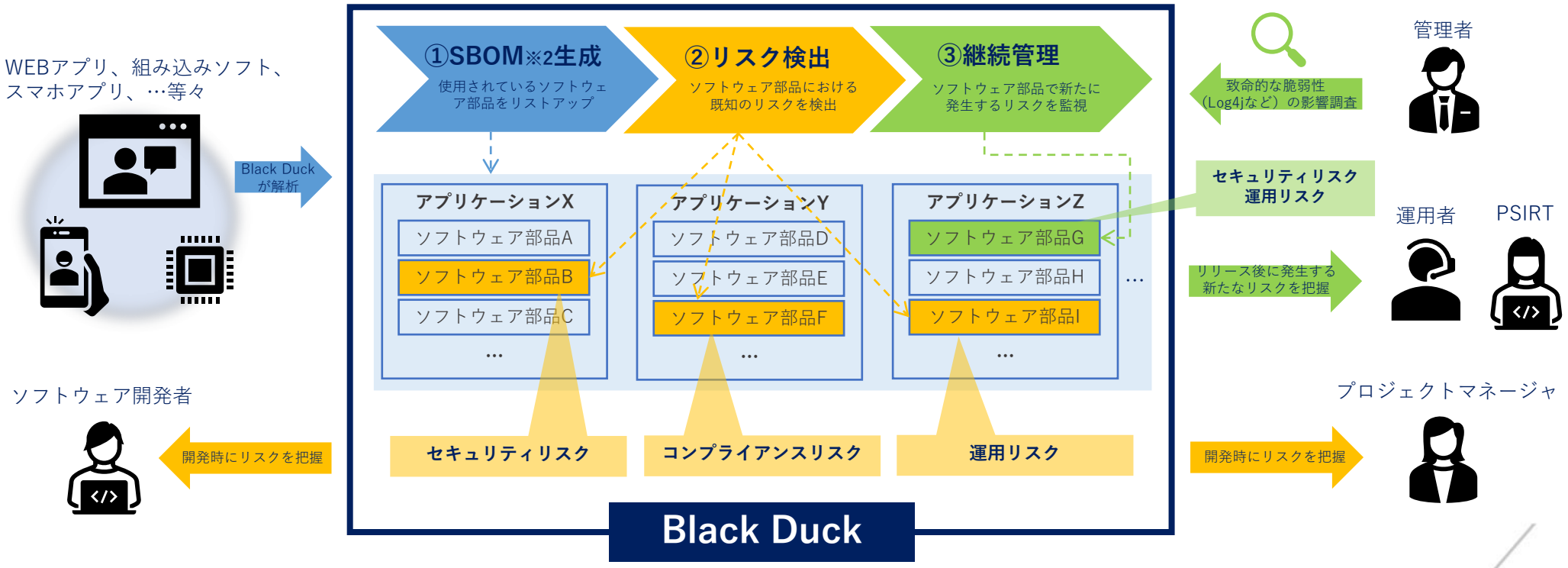
ライセンス違反による訴訟・知的財産権侵害リスク

運用リスク

EOL※1やコミュニティの活動低下などOSSの存続に関わるリスク

そういえば **Log4j** の脆弱性は対応が大変だったな…

デファクトスタンダードのBlack Duckで戦略的なOSS管理・SBOM管理を実現



株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/blackduck/

※1：End of Life（バグ対策などの改修が行われなくなった状）
※2：Software Bill of Materials（ソフトウェア部品表）

Black Duck の 特長

シフトレフト

開発プロセスに組み込んで利用できるため問題を早期に把握して修正することができます。

様々な対象を解析可能

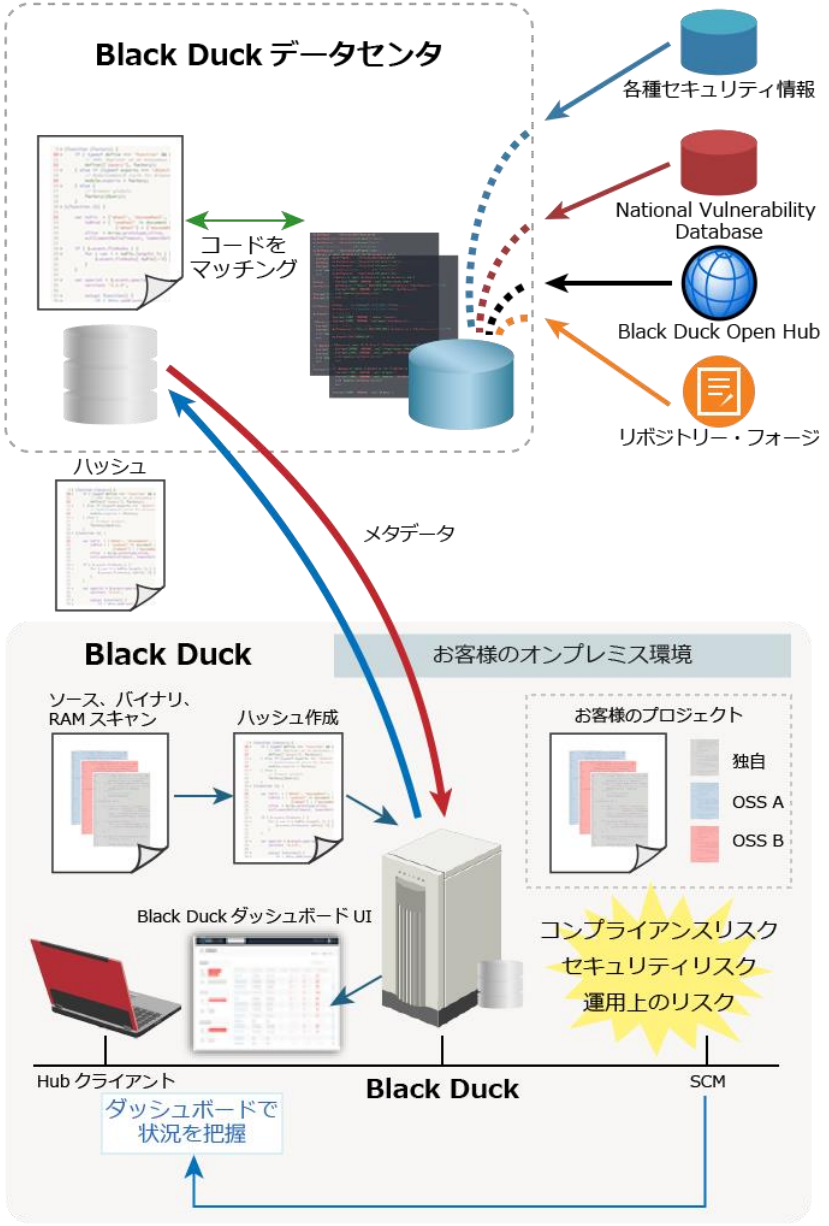
マルチファクター検出によって、あらゆるソフトウェア資産を効率的に解析できます。

包括的なリスク情報

CVEの情報だけでなく、ライセンス、コミュニティ状況、暗号など多様な情報を提供します。

迅速かつ詳細な脆弱性情報

修正方法や回避策を含んだ脆弱性情報を早期に提供しゼロデイ攻撃のリスクに対応します。



Black Duck の テクノロジー

マルチファクター検出

ソフトウェアのソースコード、パッケージマネージャ、コンテナイメージなどをもとに、コンポーネント、ファイル、スニペットなど様々な単位で使用OSS/ソフトウェア部品を洗い出します。

KnowledgeBase

世界中のオープンソースとその脆弱性、ライセンス、コミュニティなどに関する情報を保持したデータベースを備えています。確実なコンポーネント検出による正確なSBOM生成とリスク検出を可能にします。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/blackduck/