OSC2023 Online/Osaka

OSSリスク管理のススメ
～リスク管理って何すればいいの？～

2023年01月28日(土) 13:00~13:45

NEC 先端SI技術開発本部 OSS推進センター
後藤 友秀

© NEC Corporation 2022

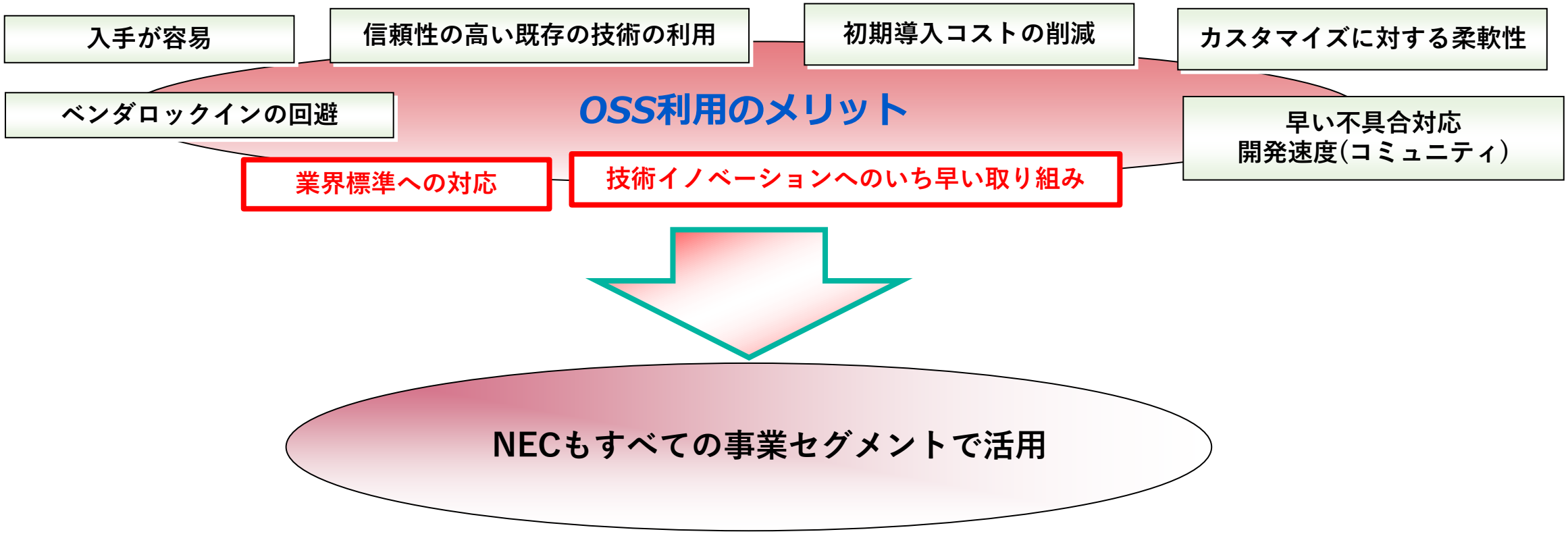
Table of Contents

OSSを取り巻く現状と利用のリスク

OSSって便利だけどなにも考えずに使っていいものなの？
OSSの利点と組みこむにあたって注意すべきリスクをしっかり把握しておこう。

多様な製品・サービスで活用されるOSS

- 多くのメリットがあり、多様な分野・業界でOSSの活用が拡大
- 今や利用しないことが競争力欠如につながる状況

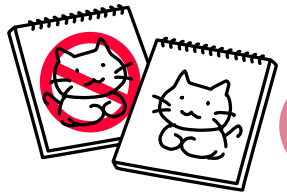


© NEC Corporation 2022

OSS利用におけるリスク

広がるOSS利用と課題

- 利用が広がる一方で、課題も顕在化。対応しきれていないケースが多数。
  - ✓ OSS利用に精通した人材不足
  - ✓ 現場判断で不用意に利用され、把握・管理不足



OSSライセンス違反による

著作権侵害・コンプライアンス問題

脆弱性の存在・対策遅れによる

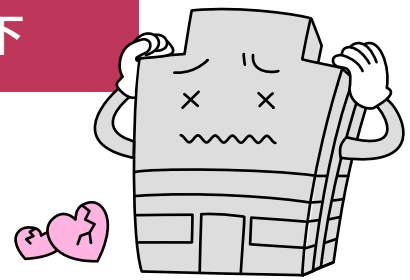
情報セキュリティ事故・情報漏洩

メンテナンス不備・バグの放置による

障害の発生・今後の製品アップデートが困難

企業の損失・ダメージ

- 刑事罰、賠償・訴訟
- 製品出荷停止の損害
- ブランドイメージの低下

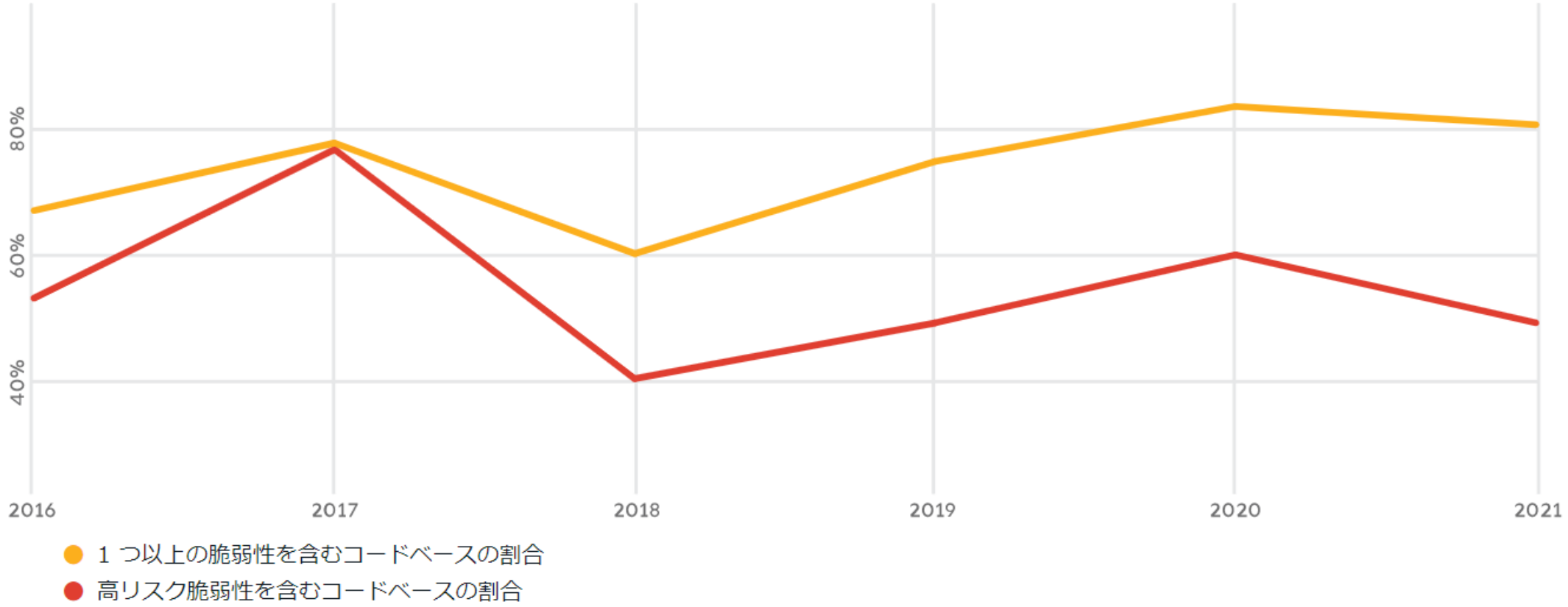


© NEC Corporation 2022

第三者情報：2021年OSSライセンス、脆弱性の状況

2,409

81



オープンソース・セキュリティ＆リスク分析レポート（2021年5月公開）.
https://www.synopsys.com/ja-jp/software-integrity/resources/reports/open-source-security-risk-analysis.html

© NEC Corporation 2022

OSSリスクマネジメントとは

開発するソフトウェアにおいて、OSSのリスク観点を検出・管理し、ライセンスリスクの回避やリリースしたソフトウェアの脆弱性対応をもれなく実施する仕組を構築しよう

OSS利用時の注意事項

現場からみたOSSのリスクや不安

管理方法・手順	
企画・開発時	**OSSの利用判断/選定の際に**、検討しているOSSのライセンス・サポート有無・脆弱性情報等の**リスクを調査**する。
開発～出荷まで	製品・サービスの**出荷まで**に、**各ライセンス条件を確実に遵守**（著作権表示・ライセンス提示・免責条項表示・ソースコード開示等を実施）していることを確認する。
開発～保守・運用	OSSの脆弱性(既存/新規問わず)などの**セキュリティリスクを開発の各段階で都度確認**する。

© NEC Corporation 2022

ライセンス違反や脆弱性をなくしたい・・あたりまえだけど、、

■ ガイドライン作って・・・とか・・・まぁいろいろ実際にはあるとは思いますが・・

ツールで自動化できるところは自動化したい。

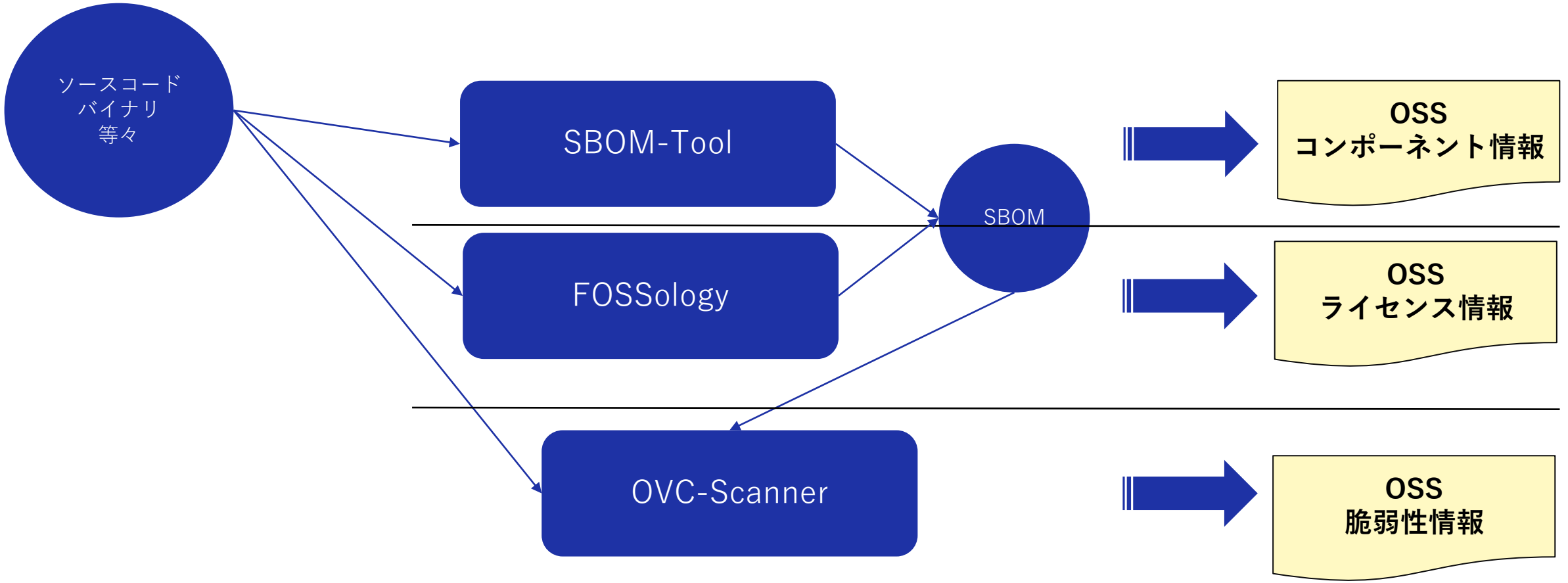
頭を使う(時間を使う)のは、検出したライセンス条項の扱いと脆弱性対応の検討だけにしたい。
(さすがにここは自動ということにはいかないか？？)

© NEC Corporation 2022

実際にやってみよう(デモ)

実際に無償ツールや有償ツールを使ってOSSリスクマネジメントをしてみよう

フリーツールでやってみる



© NEC Corporation 2022

BlackDuckを使ってやってみる

© NEC Corporation 2022

APPENDIX_A
Black Duckの概要

脆弱性・ライセンス問題の検出を実現するツールであるBlackDuckの活用を支援します。
https://jpn.nec.com/oss/blackduck-hub/

Black Duckが提供する主な機能

1. **OSSスキャン&リスト化 (= SBOM)**
   膨大なKBを基にOSSコンポーネントを認識

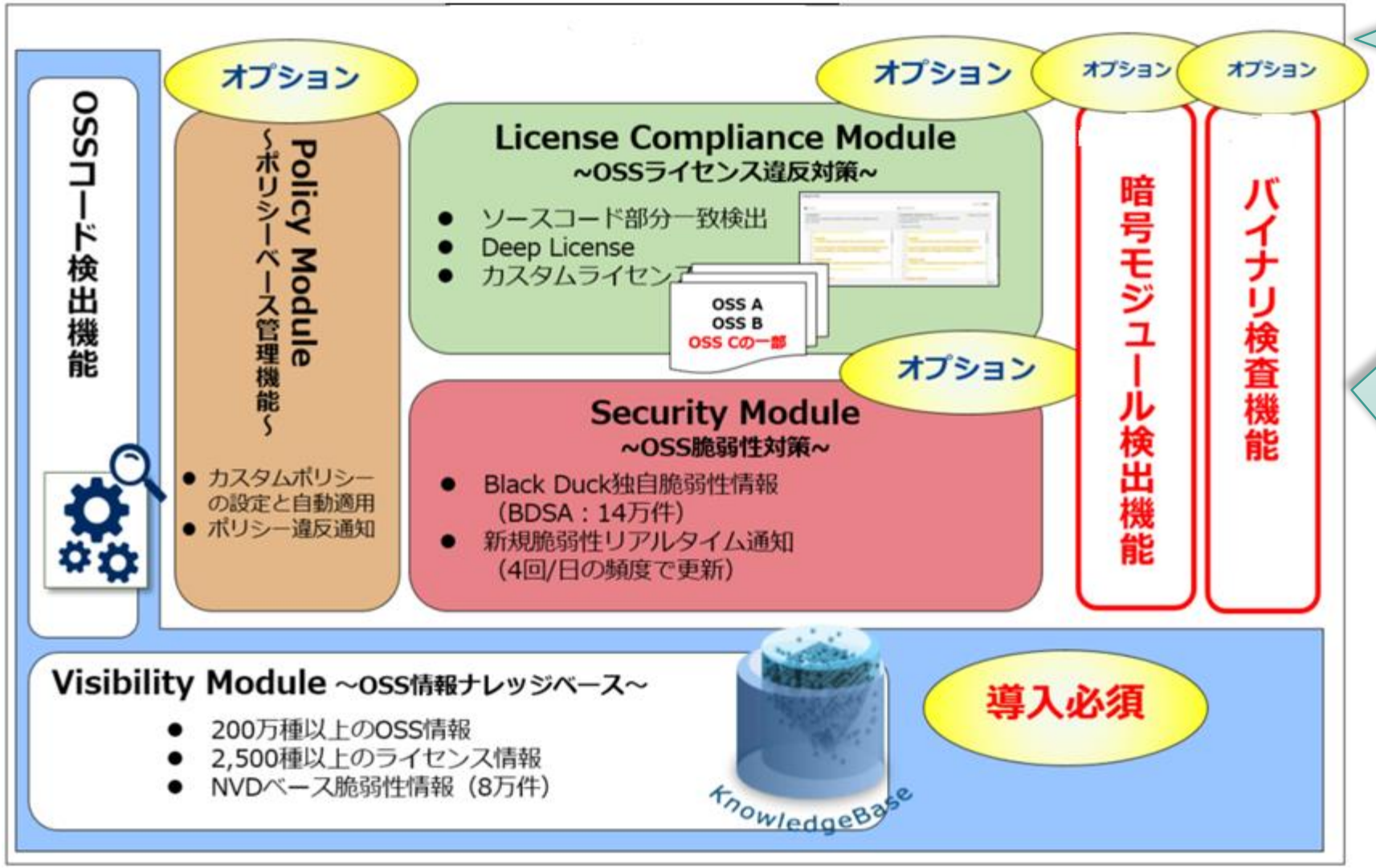
2. **リスク情報の紐付け**
   ライセンス・セキュリティ・運用のリスクを可視化

3. **対応・修正状況の管理**
   ポリシーを管理し、違反への早期対応が可能

4. **モニタ・アラート機能**
   最新の脆弱性をウォッチし、アラートを発信！

© NEC Corporation 2022

Black Duckが提供する主な機能



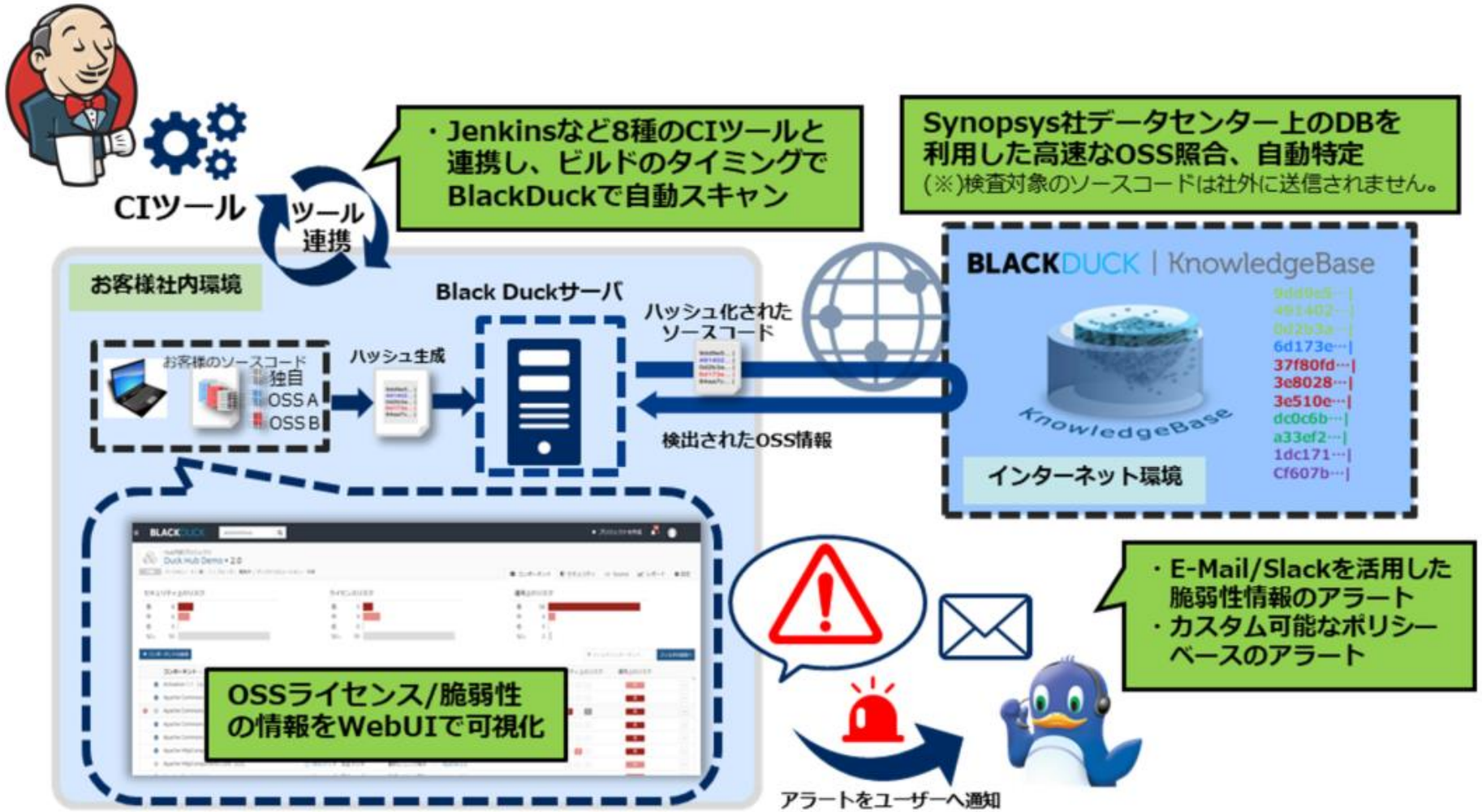
必要な機能を事業の用途に合わせて、自由に組み合わせることが可能！

■豊富な連携プラグイン（Integrations）

CIツールをはじめ、パッケージマネージャ、IDE、リポジトリマネージャなどといった、様々な開発支援ツール群と直接連携。開発シーンに合わせた形で統合。

© NEC Corporation 2022

Black Duckが提供する主な機能



"Jenkins logo" by jenkins.io(https://jenkins.io/) is licensed under CC BY-SA 3.0

© NEC Corporation 2022

顧客課題を解決するNEC商流BlackDuckサポートの強み

BlackDuck機能

- **OSSスキャン&リスト化**
- **リスク情報の紐付け**
- **対応・修正状況の管理**
- **モニタ・アラート機能**

NEC強み

トータルソリューション提案力

- HW・OS・AP一気通貫サポートのトータルソリューション（Linuxプラットフォームはシェア国内トップクラス）

活用ノウハウ

- 自社でのBlack Duck活用実績(10年以上)
- 高品質のサポート＋導入支援、解析支援

OSSライセンスコンサル

※製品サポートと独立提供

- ネットに散在する都市伝説に惑わされないOSSライセンスの正しい理解、正しい判断ができる組織育成を支援。

© NEC Corporation 2022

APPENDIX_B
OSSライセンスコンサルティング

OSSライセンスに関する正しい理解、判断ができる組織育成を支援します。
https://jpn.nec.com/oss/osslc/

OSSライセンスコンサルティング

■ コンサルティング・メニュー

弊社HPより抜粋

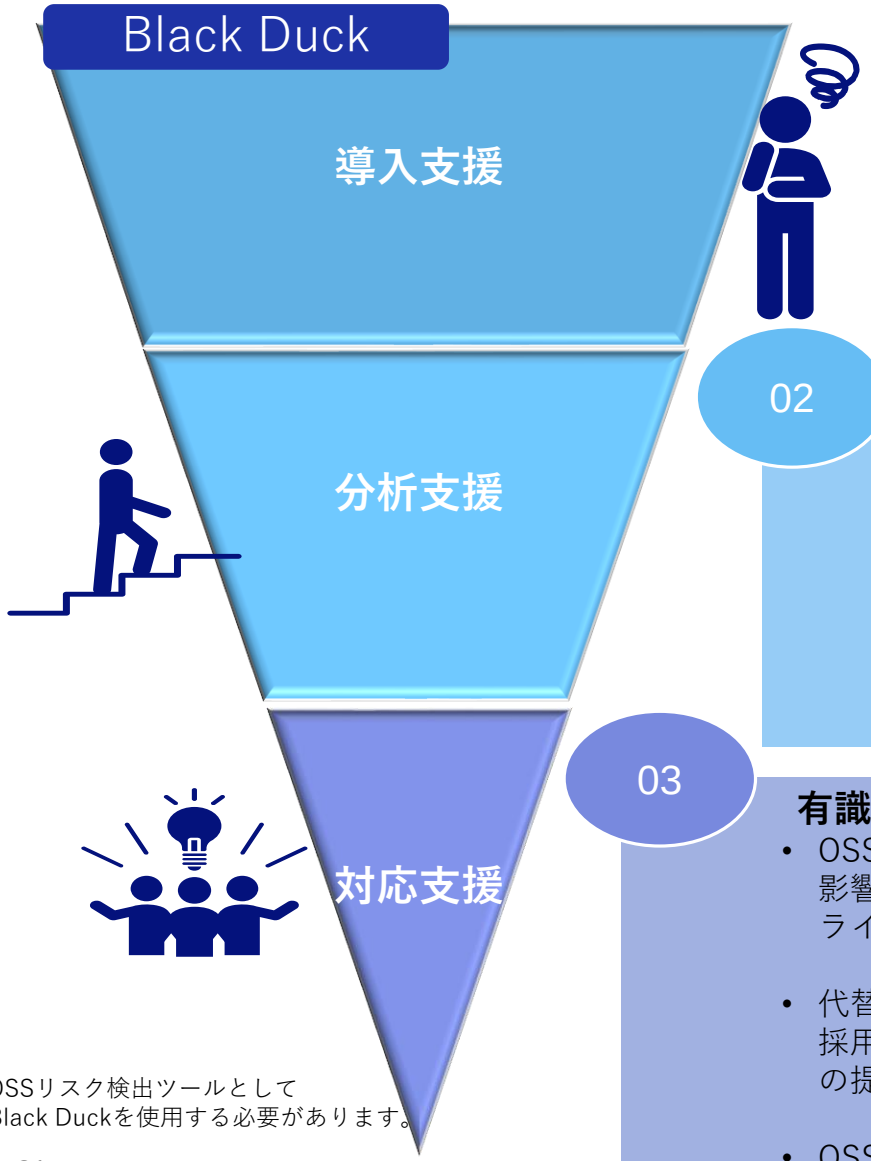
ご要望	ご推奨サービス
理解レベルのコンサル a. OSSライセンスは条文を眺めただけでは分かりません。 根拠となる著作権法から順にお話します。	OSSライセンスと著作権法 講義
ケーススタディでのコンサル b. 実製品での利用OSSを例に、OSSライセンスの正しい理解の仕方・対策のガイドラインの作成をご支援します。	OSS利用ガイドライン作成支援
開発プロセスレベルのコンサル c. ガイドラインに沿った運用を確認できる帳票を導入したプロセスに改善したい	開発管理プロセス改善支援
d. 従来物件でのOSS利用状況を調べたい。 新規物件でのOSSを流用・包含していないことを確認したい	Black Duck
推進活動のコンサル e. OSS利用申請書を導入し運用した場合、判断に迷う場合にアドバイスがほしい 運用に入ってからもガイドラインの拡充のために雛形を作成してほしい	活動支援アドバイス・サービス
特定製品のコンサル f. OEM製品など開発済み物件の対応状況の妥当性について、個別に相談したい	製品個別・対策支援アドバイス・サービス

© NEC Corporation 2022

APPENDIX_C
OSSリスクマネジメント支援サービス

BlackDuck活用により検出した脆弱性やライセンス問題について分析や対策を支援します。
https://jpn.nec.com/oss/blackduck-hub/rel_prod.html

OSSリスクマネジメント支援サービス



※OSSリスク検出ツールとして
Black Duckを使用する必要があります。

01

環境構築コンサルティング
- OSSライセンスリスク・脆弱性検出環境の構築支援
- リスク検出の仕組み運用支援(CI/CDへの組込みなど含む)

試行プロジェクトのレポートによる分析手順コンサルティング
- サンプルを元に検出内容の観点や解析手順コンサルティング

02

SBOM対応
- 採用OSSの特定/整理
- 各種レポート(OSS名、Ver.情報、OSSライセンス、既知の脆弱性、コミュニティ状況) の出力と分析レポートの作成

OSS頒布の際に有効な情報提供コンサルティング
- SPDXレポート、著作権データレポート、採用OSSのライセンス条項提示、etc.

03

有識者による出荷リスク検証・解析支援
- OSSライセンス対応支援
  影響範囲の切分け支援、競合診断、スニペットマッチの目視判定、解析による採用OSSの精査、不明な独自ライセンスの調査、etc.
- 代替OSS・代替バージョン提示、OSSコミュニティの健康状態の診断、OSSのサポート期間に応じたOSSの採用リスク判断、その他OSSライセンスに関する相談、etc.（代替OSS、バージョン提示は候補となるOSSの提案であり、開発物件での確実な動作保証をするものではありません）
- OSSが保有する脆弱性の解決支援

© NEC Corporation 2022

ぜひ！お問い合わせください！

- ご清聴いただき、有難うございました。
- 今日の話を聞いて、ちょっと相談してみようかなと思ったかた・・・
- ぜひ！下記アドレスまでご連絡ください！

blackduck-info@osspf.jp.nec.com

- OSCでちょっと話聞いたんだけど！っと本文に入れていただけると後藤が喜んで返信いたします。

© NEC Corporation 2022

ご清聴いただき、有難うございました。

© NEC Corporation 2022


Orchestrating a brighter world
NEC