Empowered by Innovation NEC

「思わぬ流用」を見逃していませんか？
OSSコード検出ツール「Black Duck Protex」活用のすゝめ

2010年5月19日
NEC 第一ITソフトウェア事業部
山本

Contents

Black Duck Protex

1. 背景

2. 機能・作業フロー

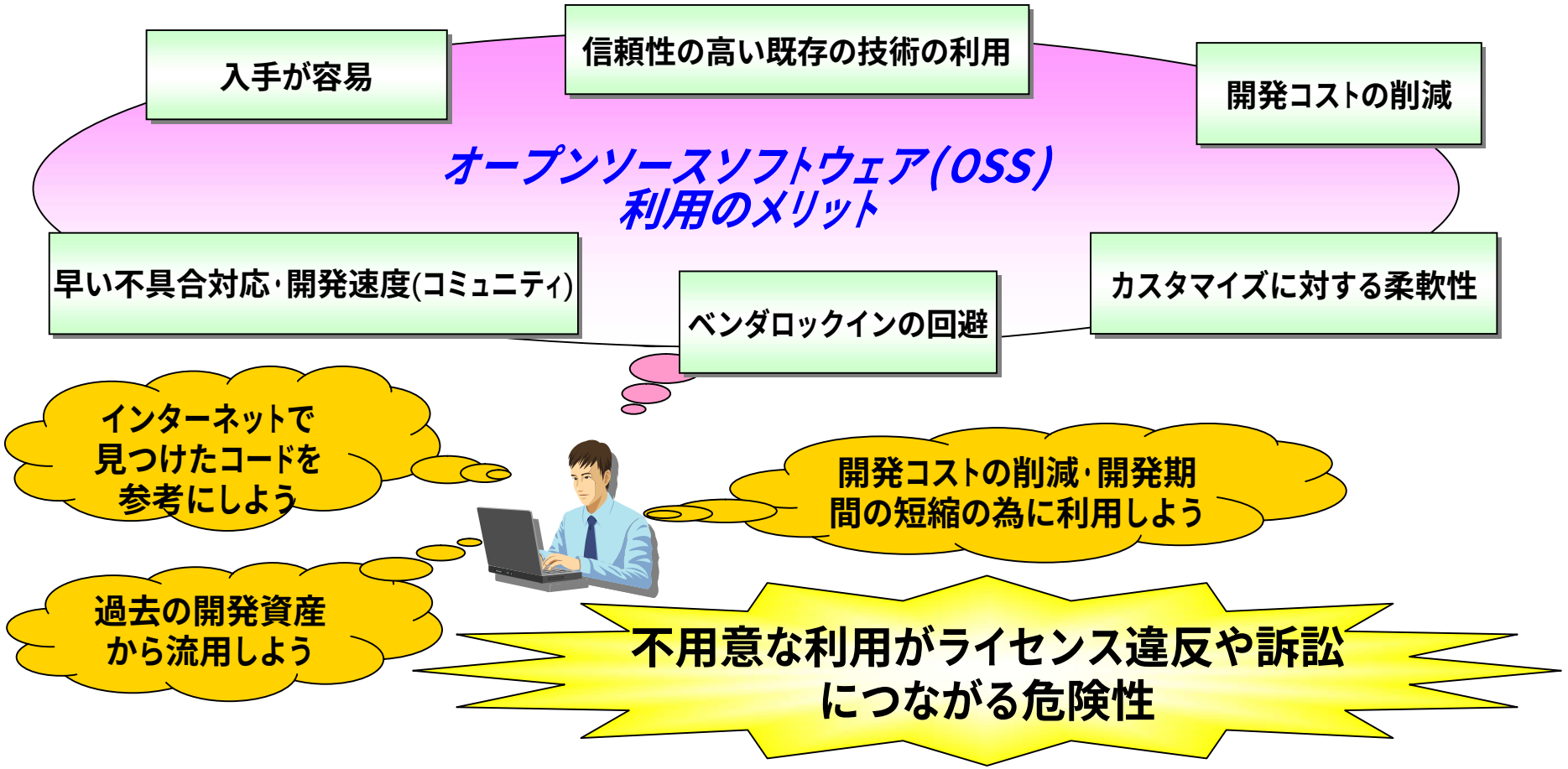
3. 製品・サービス体系

1. 背景

OSS利用のメリットと注意点

Black Duck Protex

- OSS利用にはさまざまなメリットがありますが、入手・再利用の容易性から安易に流用されがちという側面もあります。
- OSSは利用の際守るべきライセンスがありますが、不十分な理解・検証が原因でライセンス違反を起こす事例が多数発生しています。



違反の代償は甚大

Black Duck Protex

過去訴訟で実際に課された条件

① 和解金（金額は非公開）

② OSSライセンスコンプライアンス責任者の設置

③ GPL遵守：ソースコード公開と顧客への告知

- ✓ 損失は含まれる自社IPに依存。潜在的に非常に高いリスクあり。

④ 出荷差し止め・延期（製品改修）

- ✓ 開発規模・事業規模に依存。潜在的に非常に高いリスクあり。

訴訟に至らず(Webでの指摘や批判等)ともダメージは大差無し

- 上記③④は自主的な実施が不可避となる可能性大

いずれのケースでも…

⑤ ブランドイメージの低下

- ✓ 他事業への影響、取引先からの信頼失墜で契約解除…プライスレス！

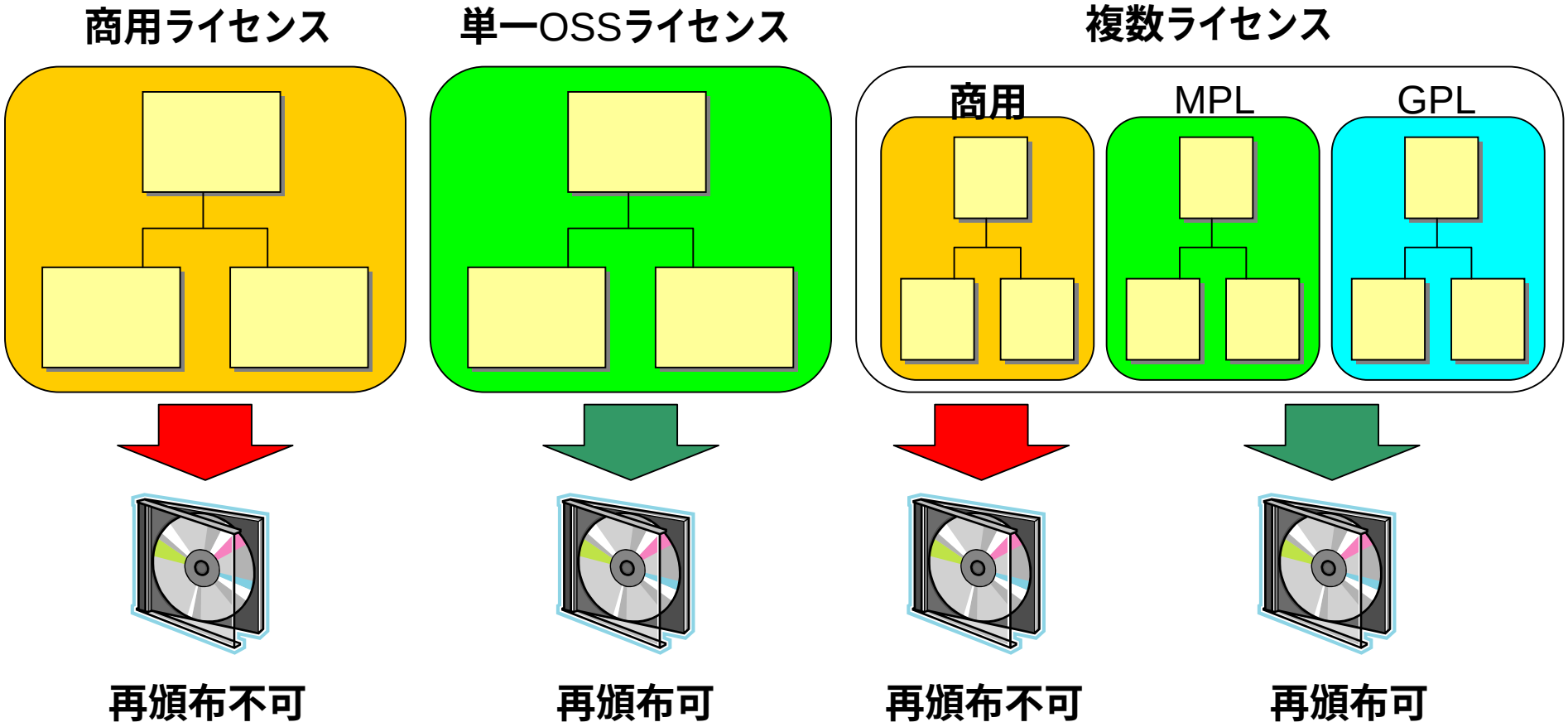
対象となった製品・事業規模によってはこれらの代償は計り知れず、事業や会社そのものの存続に関わる事態にもなりかねません。

ライセンス違反を起こさないために①

Black Duck Protex

◆ ライセンスを意識した開発管理･構成管理
- ✓ それぞれのライセンス要件を遵守
- ✓ リリース媒体を分けるなど分かりやすい出荷形態

企画･設計段階での OSSポリシー策定



OSS License Checked!

Empowered by Innovation NEC

「思わぬ流用」はなぜ起きるのか？

Black Duck Protex

よくある誤解

うちの製品にはOSSを使っていないから
コード検査の必要はないでしょう？

いいえ。

OSSを使っていないつもりのプロプラ製品でこそ
「思わぬ流用」への備えが必要です。

「思わぬ流用」の要因

なぜ？
開発標準・品質基準など
の統制が行き届きにくい

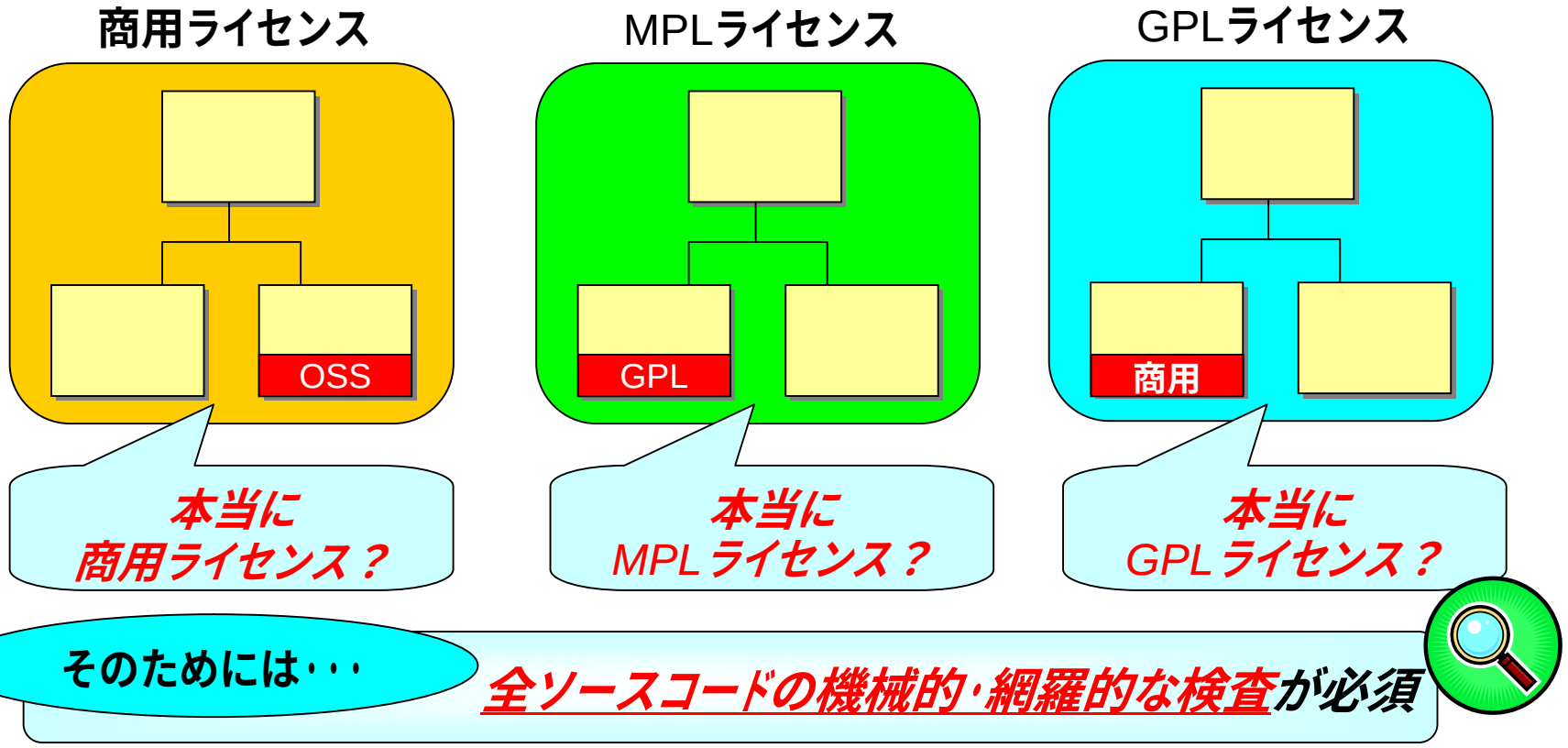
- ✓ *過去資産の不用意な再利用*
- ✓ *外注・オフショア納品物件*
- ✓ *テスト用コード、研究所のサンプル実装などの削除忘れ*

ライセンス違反を起こさないために②

Black Duck Protex

◆ 各開発物件に他のライセンスのプログラムが混入していないことを確認
- ✓ 安易な流用、意図しない混入を検出
- ✓ 外注先やオフショアからの納品物件を受け入れ検査

策定したOSSポリシーと実装が一致していることを確認



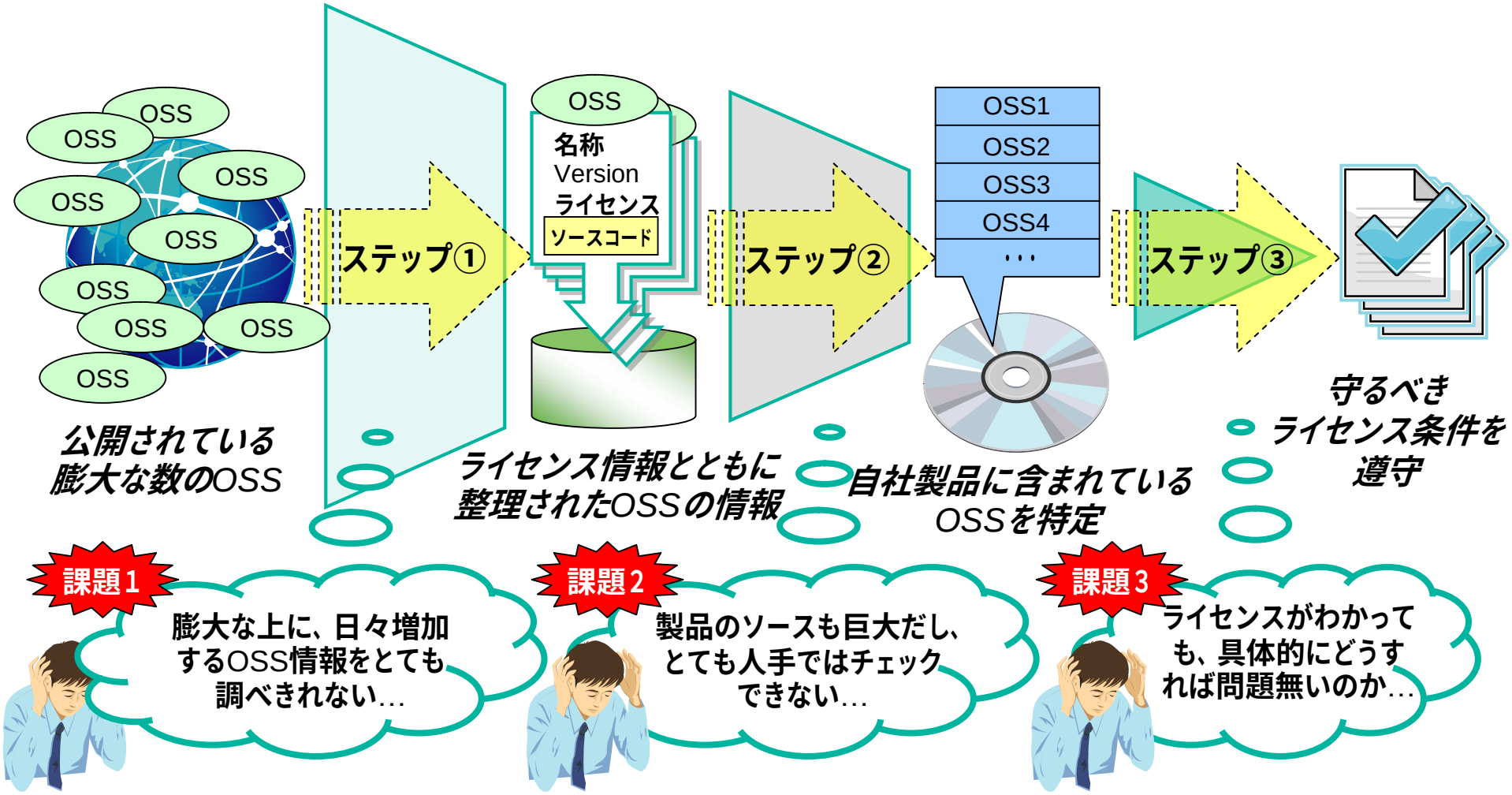
そのためには・・・ ***全ソースコードの機械的・網羅的な検査が必須***

OSS License Checked! Empowered by Innovation NEC

課題は何でしょうか？

Black Duck Protex

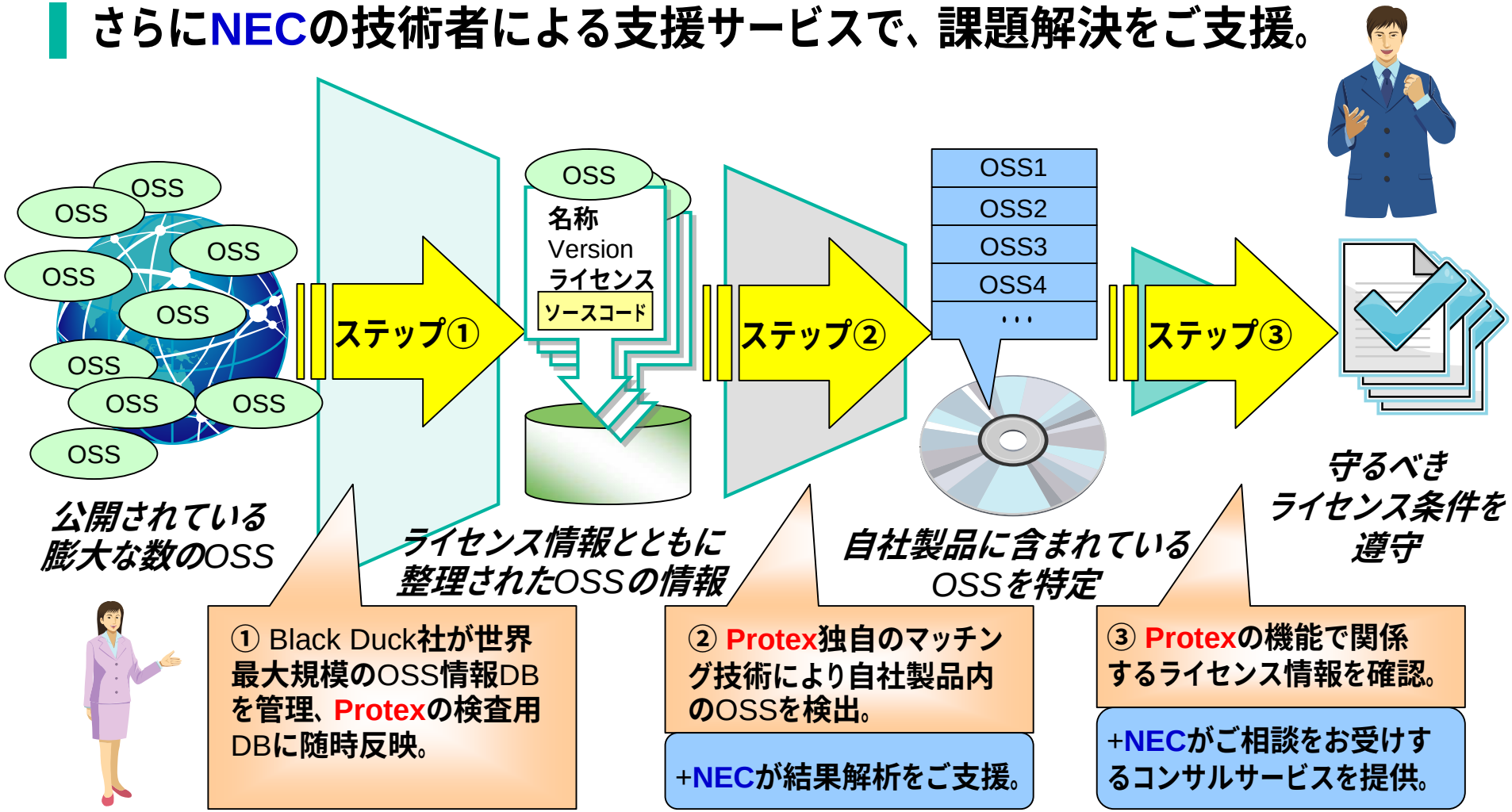
検査のために必要な各ステップから考えてみましょう。



私達がお手伝いします！

Black Duck Protex

- 「Protex」が機械的・網羅的な処理を実行。
- さらにNECの技術者による支援サービスで、課題解決をご支援。



OSS License Checked!

Empowered by Innovation NEC

2. 機能･作業フロー

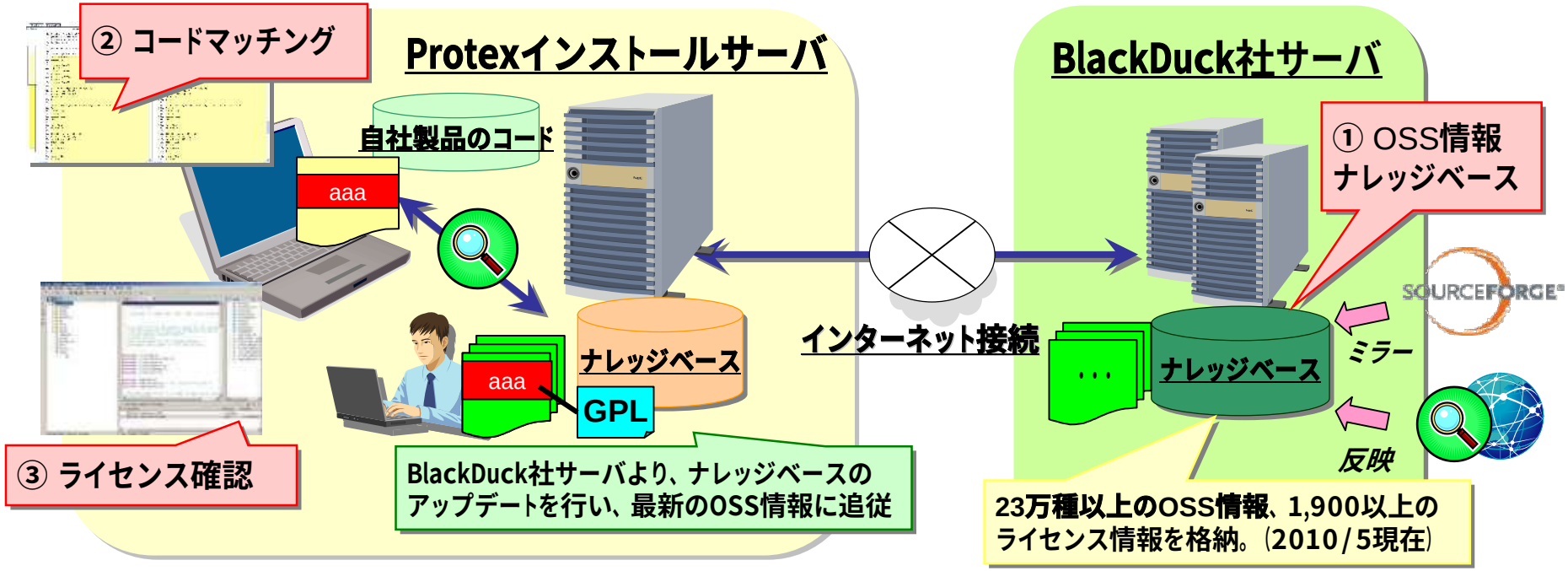
機能概要

Black Duck Protex

① **OSS情報ナレッジベース**
著名なOSSリポジトリサイトをミラー、その他ネット上のOSS情報を日々チェックし反映。

② **コードマッチング（Analysis）**
自社製品のコードとOSSコードを比較し、一致または類似箇所を検出。
バイナリファイル（ライブラリ、アイコン等）の一致も検出。

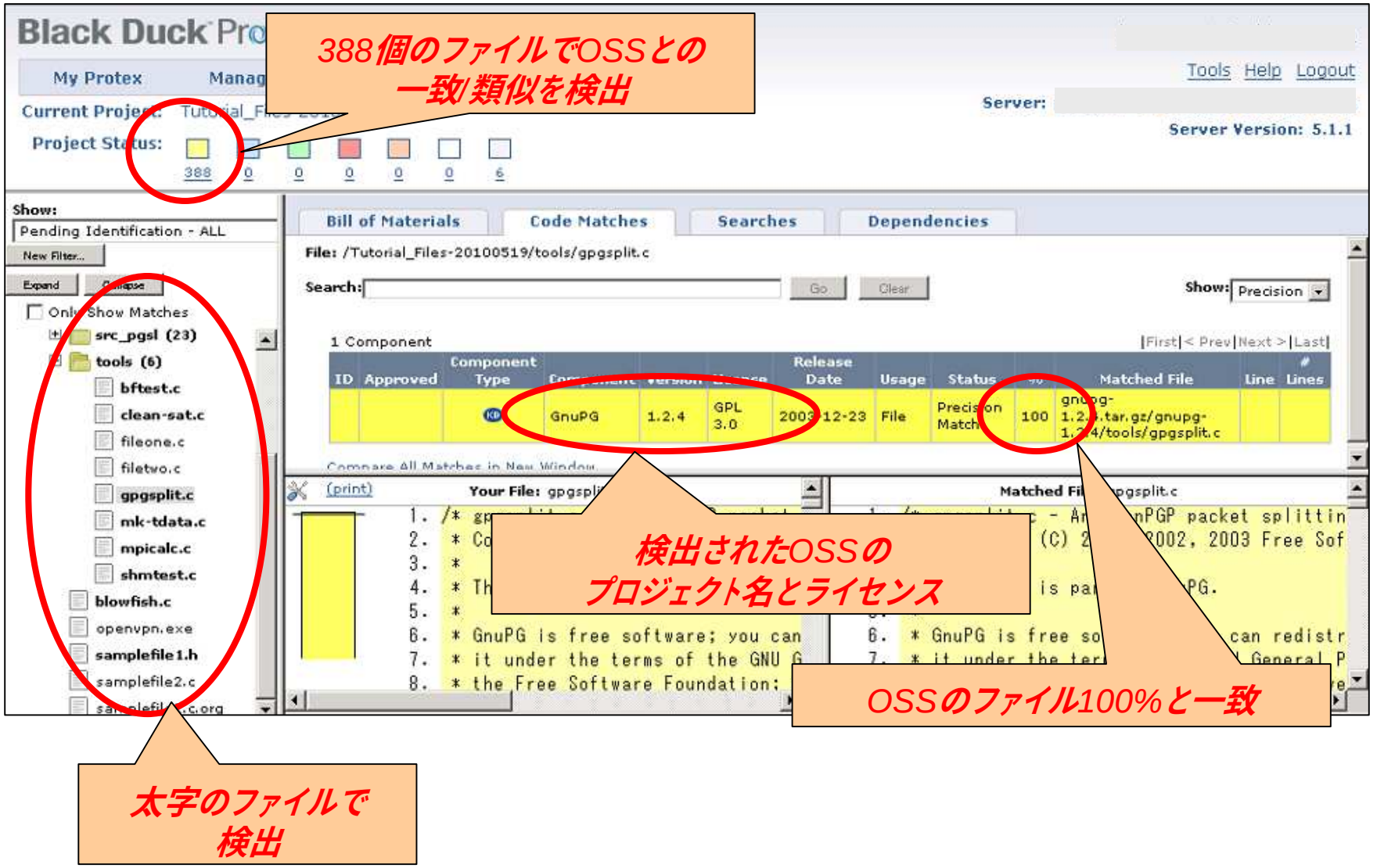
③ **ライセンス確認**
検出されたOSSのライセンスを確認。自社製品のライセンスと互換性の無いライセンスは警告表示。



OSS License Checked! Empowered by Innovation NEC

Analysis結果からわかること

Black Duck Protex



OSS License Checked!

Empowered by Innovation NEC

Protexをお勧めする3つの理由

Black Duck Protex

①強力なOSS情報ナレッジベース

②高精度のマッチング機能

③多様なカスタマイズを可能にする拡張機能

特長① 強力なOSS情報ナレッジベース

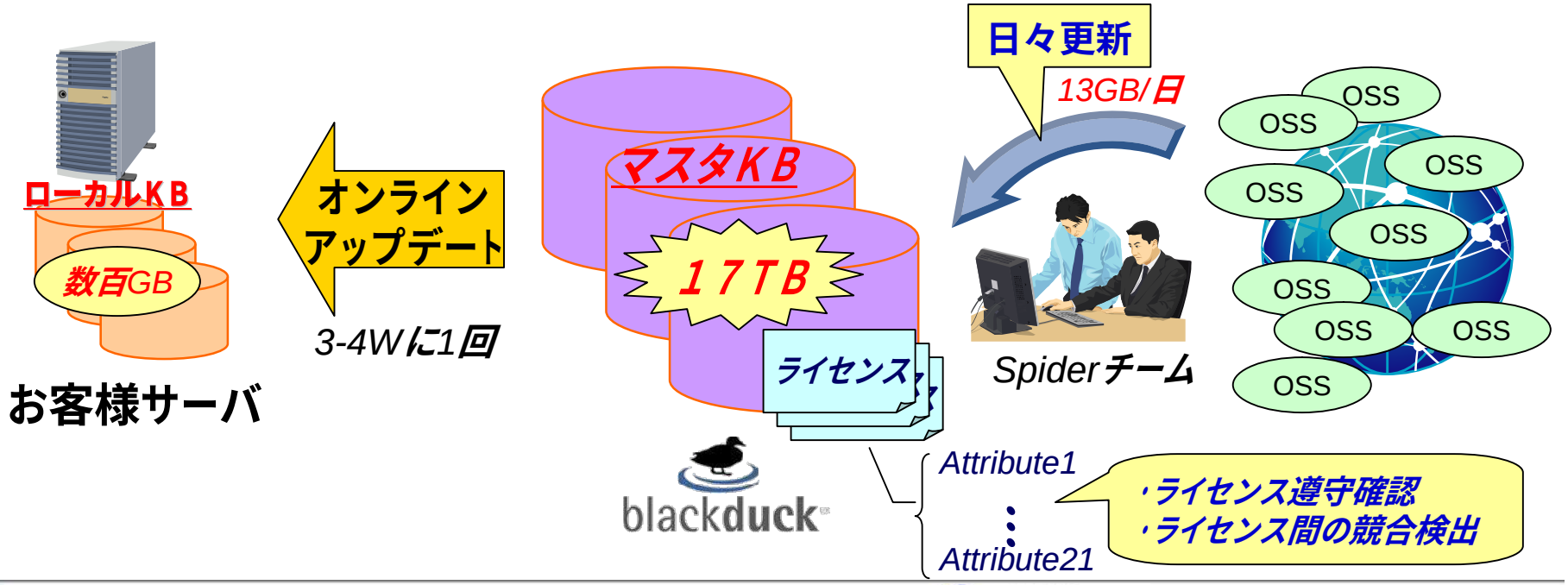
Black Duck Protex

■ 世界最大規模のOSS・ライセンス情報DB

(※) 2010年5月現在 23万種以上のOSS、1,900以上のライセンス情報を格納。
総データサイズ17TB。平均13GB/日で新規情報を追加。

■ ソースコードだけでなくバイナリ(ライブラリ、アイコン等)も格納

■ お客様サーバは自動オンラインアップデート



OSS License Checked!

Empowered by Innovation NEC

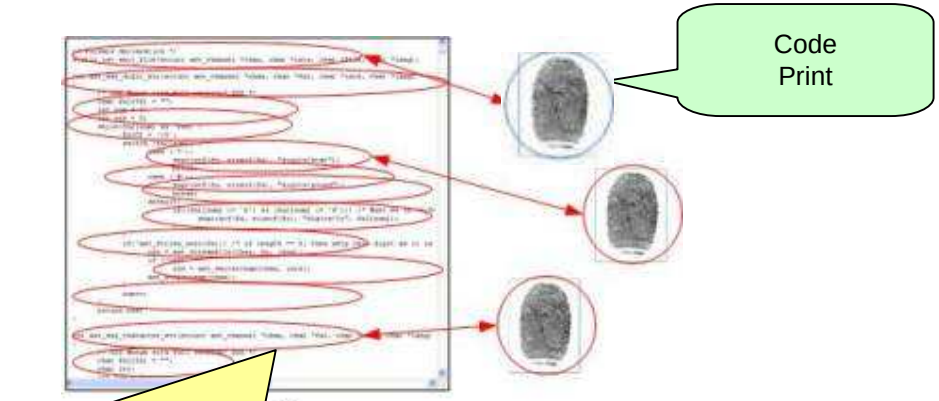
特長② 高精度のマッチング機能

Black Duck Protex

■ コードの特徴を抽出・エンコードするCode Print技術
- ✓ データサイズの大幅な縮小、高速な照合を実現。

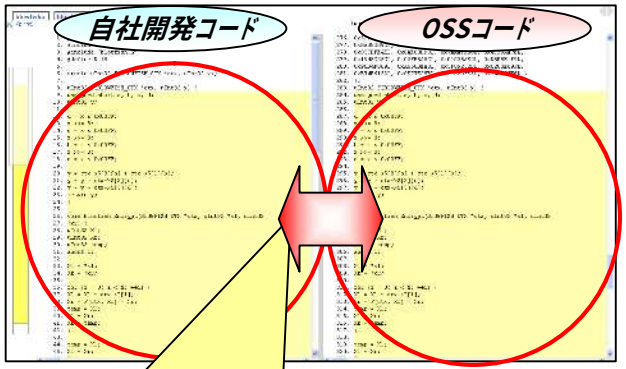
■ ソースコードの「思わぬ流用」も高精度で検出
- ✓ ファイル単位の流用はもちろん、コードの一部流用にも対応
- ✓ 一部改変を伴う流用も類似していれば検出（悪意のある改竄にも効果）

■ 自コードとOSSの対比表示機能
- ✓ 流用箇所、改変部分が一目瞭然



コード断片レベルで照合し
類似箇所を発見

対比画面



一致・類似箇所はハイライト表示

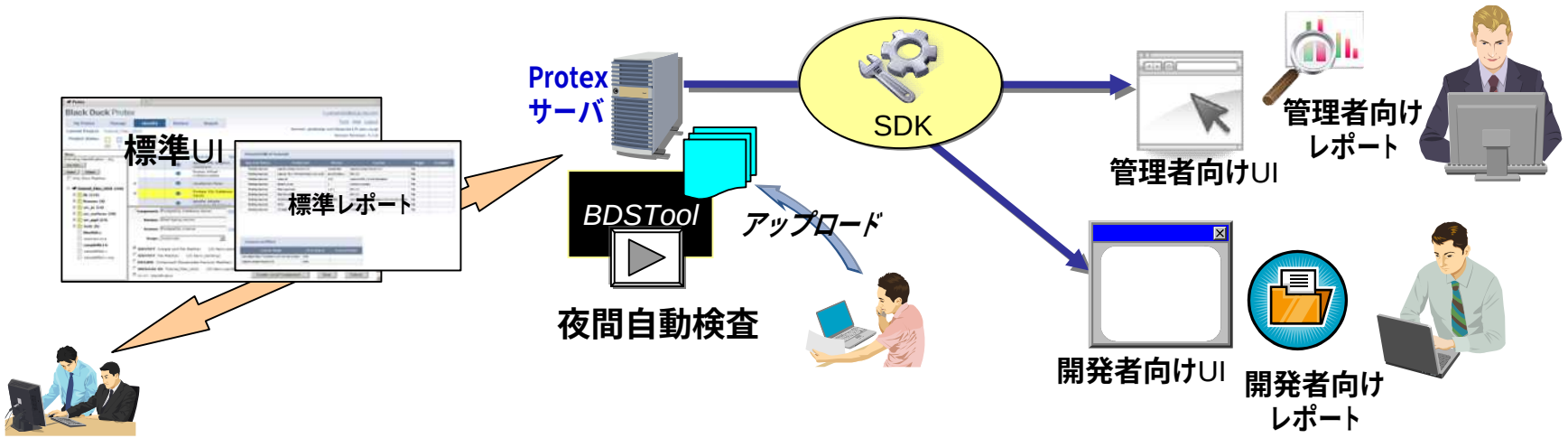
特長③ 多様なカスタマイズを可能にする拡張機能

Black Duck Protex

■ **カスタムナレッジベース**
- ✓ ユーザ独自コードやライセンス定義をナレッジベースに追加登録

■ **コマンドラインインタフェース** (BDSTool)
- ✓ コードマッチングをコマンドラインから実行
- ✓ バッチファイル、スクリプトによる自動検査が可能

■ **SDK** (オプション)
- ✓ Protexの各機能を呼び出すAPI群
- ✓ Java、C#、Perl、Pythonで利用可能
- ✓ カスタムUI・カスタムレポートなど柔軟な実装を実現



OSS License Checked!

Empowered by Innovation NEC

3．製品･サービス体系

製品・サービス体系

Black Duck Protex

➢ 製品ライセンス、サポートサービス、付加サービスで構成

個別見積

③ NEC付加サービス

・導入支援サービス

インストール、構築作業、基本トレーニング

・解析支援サービス

コード検査結果の確認作業をご支援

コンサルティングサービス もご用意。

② NECサポートサービス

・TEL、E-Mail、FAXによる製品使用方法のQ&A、障害調査

・Web、mailによる情報提供

価格はご相談ください

バンドル

① 製品ライセンス (年間Subscription)

・ 製品使用 (サーバ1台あたり1ライセンスが必要)

・ Rev.up権、ナレッジベース更新権

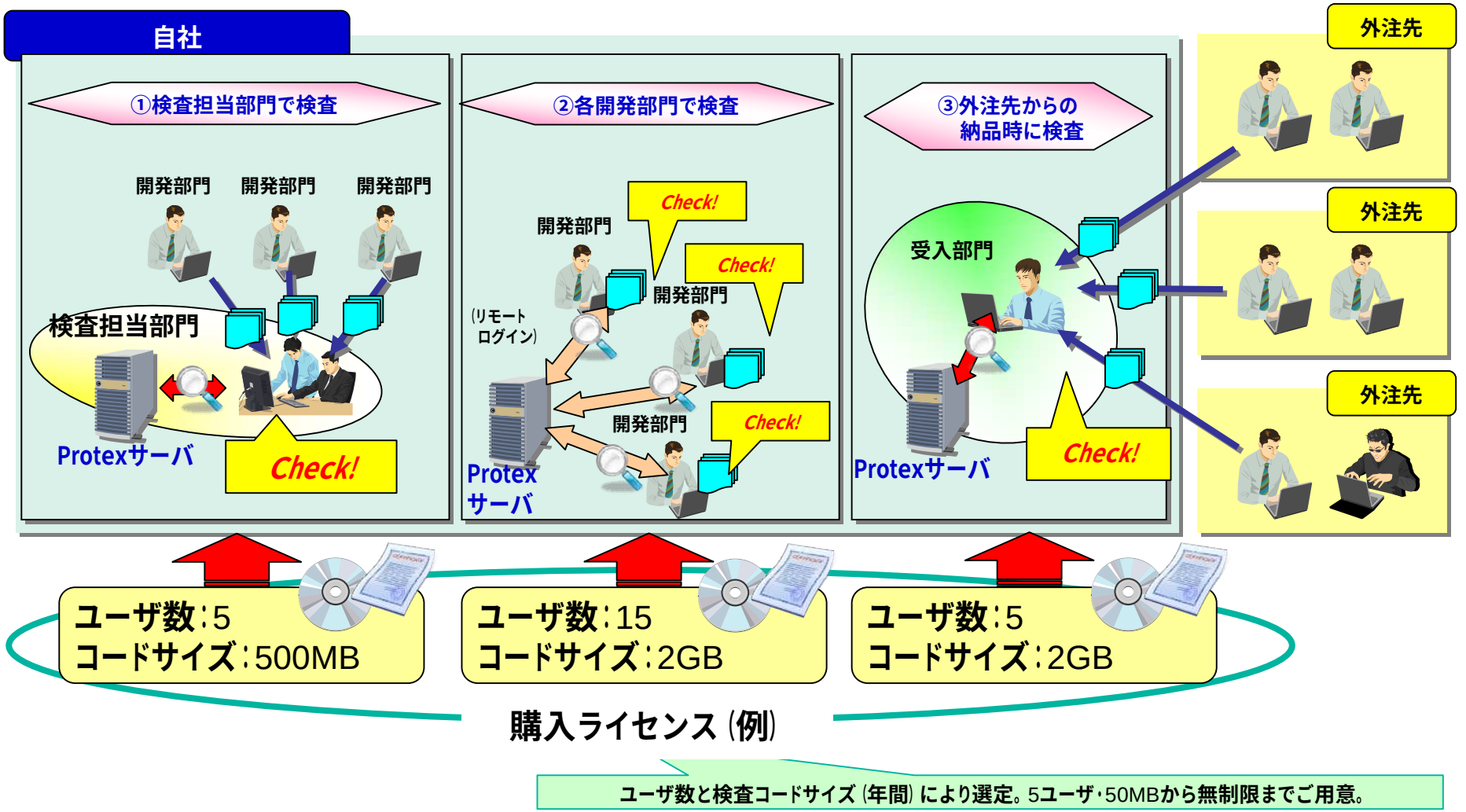
・ユーザ数、検査コードサイズ (年間) 別の価格設定

スポットサービス もご用意。

導入パターン

Black Duck Protex

お客様の開発/品質管理体制・組織構造に応じ、様々な導入パターンが可能。

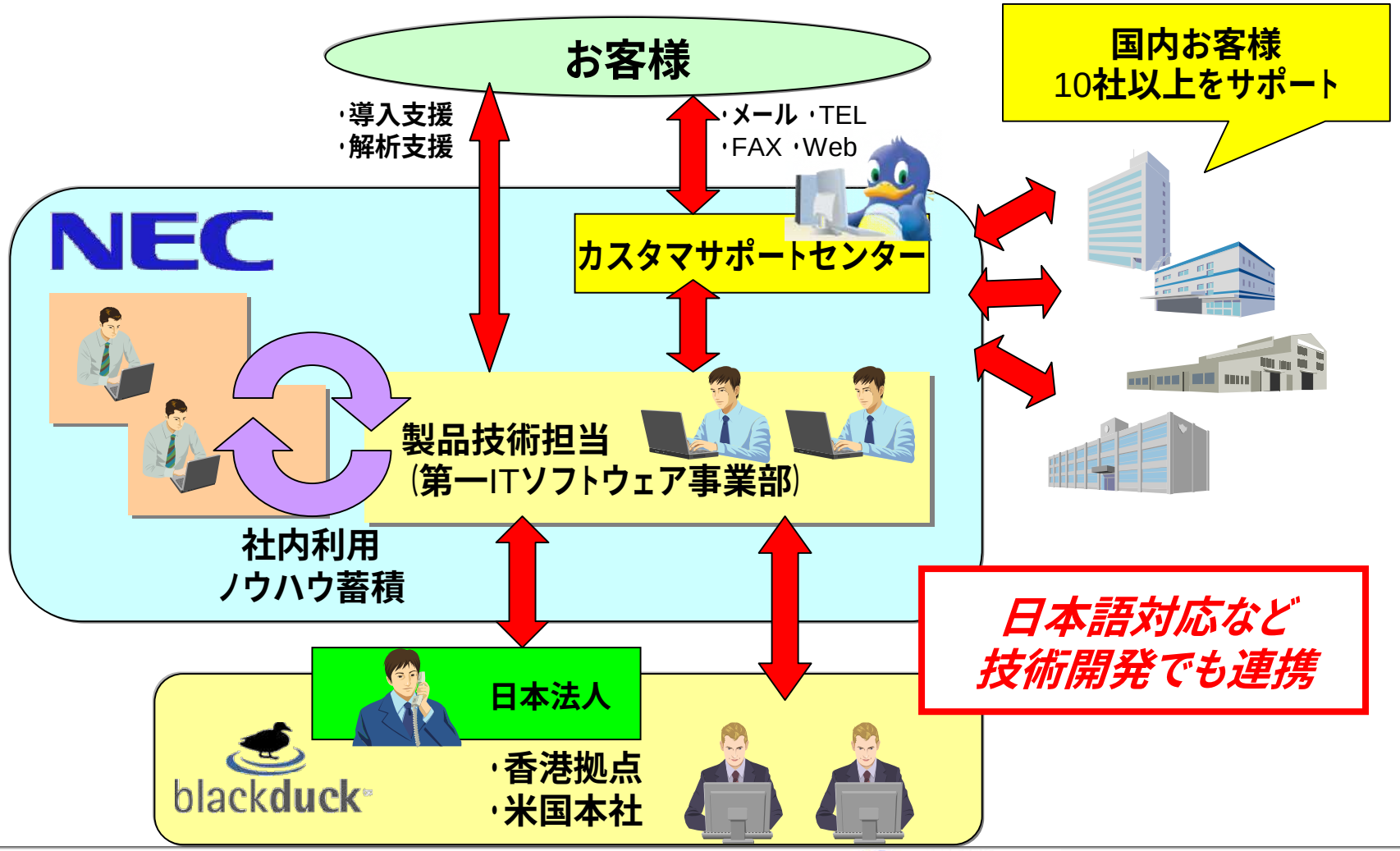


ユーザ数と検査コードサイズ(年間)により選定。5ユーザ・50MBから無制限までご用意。

国内サポート体制

Black Duck Protex

自社利用で蓄積したノウハウ、開発元Black Duck社との密連携により
日本のお客様に安心のサポートをご提供



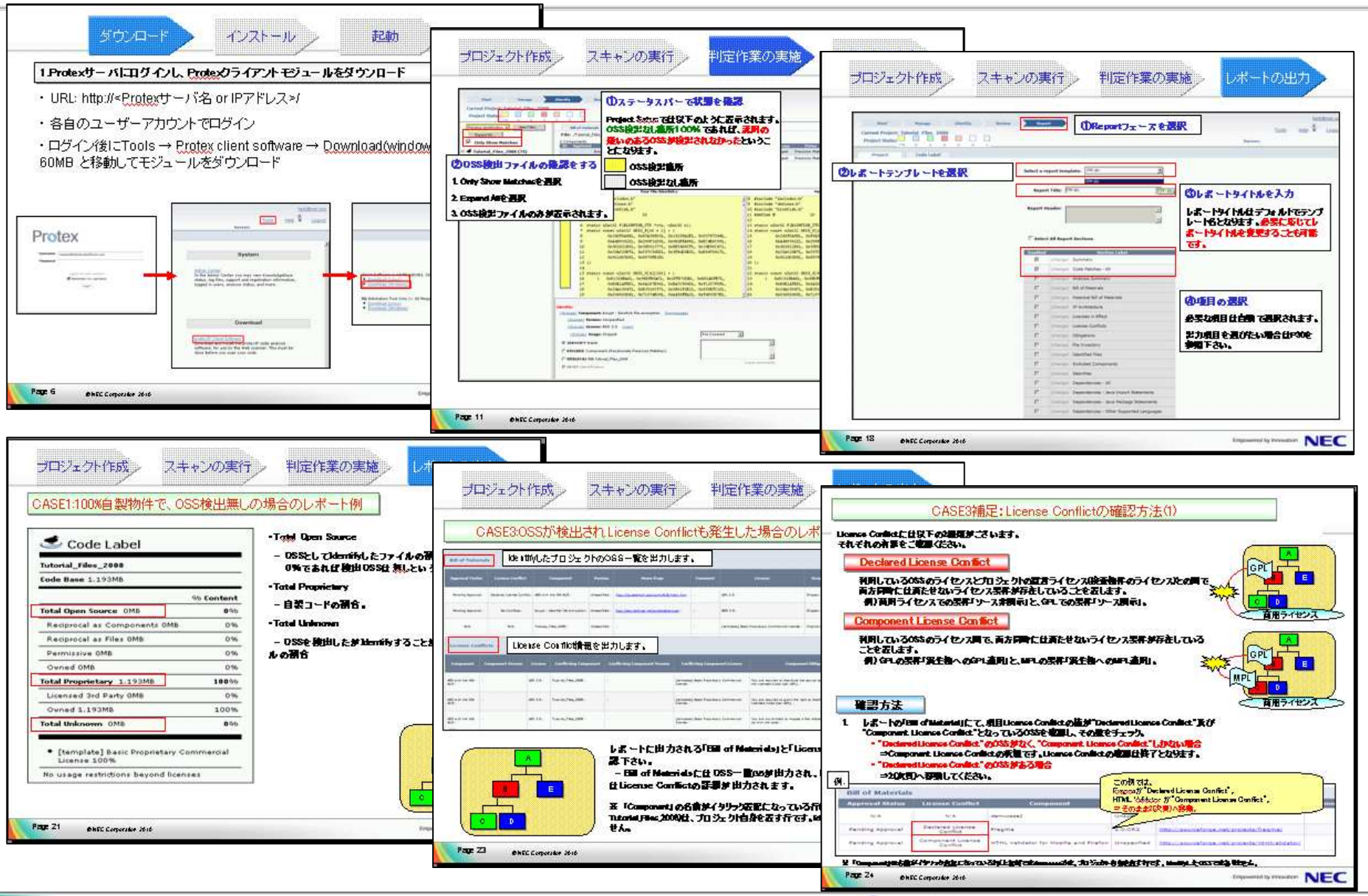
OSS License Checked!

Empowered by Innovation NEC

ご参考

導入支援資料「利用ガイド」(NEC作成)

Black Duck Protex



OSS License Checked!

Empowered by Innovation NEC

無料体験のご案内

Black Duck Protex

① お試し版レポート、② 評価ライセンスの2種類をご用意。

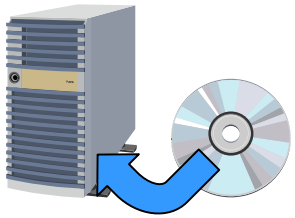
①お試し版レポート

- お客様のソースコード（最大25MB）をお預かりし、スキャン結果をお返しします。
- 正規製品の出力との差分はありません。
- 機材のご準備は不要です。

どのような結果が得られるかをお手軽に確認したい方はこちら

②評価ライセンス

- 最長30日間、25MBまで、製品をご試用いただけます。
- 正規製品との機能差分はありません。
- 別途評価用サーバ、OSが必要です。



詳細な機能をじっくりとお試しになりたい方はこちら

ご希望の方は担当者まで！

ご参考

～組込みシステムソリューション～

ソースコード第三者検証サービス

Black Duck Protex

- ソースコードに潜む問題（バグ）をご報告します。
- 複数静的検証ツールによるチェック結果を専任解析者が解説したレポートをご提供します。
- お客様システムの品質向上と開発効率化に貢献します。
- 対象言語：Ｃ言語／Ｃ＋＋／ＪＡＶＡ

有効性

■短期開発／技術者不足の時に
- ●高品質なソフトウェアを提供したい
- ●ソースコードレビューそのものをアウトソーシングしたい

■構外請負の品質管理を向上したい時に
- ●ソフト品質を同一基準で数値的に把握したい
- ●受入試験中に重大問題に遭遇したくない

■開発者に負荷をかけたくない時に
- ●ツール導入時のリソースが一切不要
- ●開発者へのツール使用方法の教育不要

実績

■延べ８００件以上のプロジェクトに適用
■検証サービス実施の総規模は800,000KLine以上（過去３年間の実績値）

サービスの流れ

OSS License Checked!

Empowered by Innovation NEC

製品情報･お問い合わせ

Black Duck Protex

- **製品情報**
  http://www.nec.co.jp/oss/protexip/

- **お問い合わせ**
  E-Mail：protexip-info@osspf.jp.nec.com
  （NEC 第一ITソフトウェア事業部 Protex担当）

Empowered by Innovation