



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

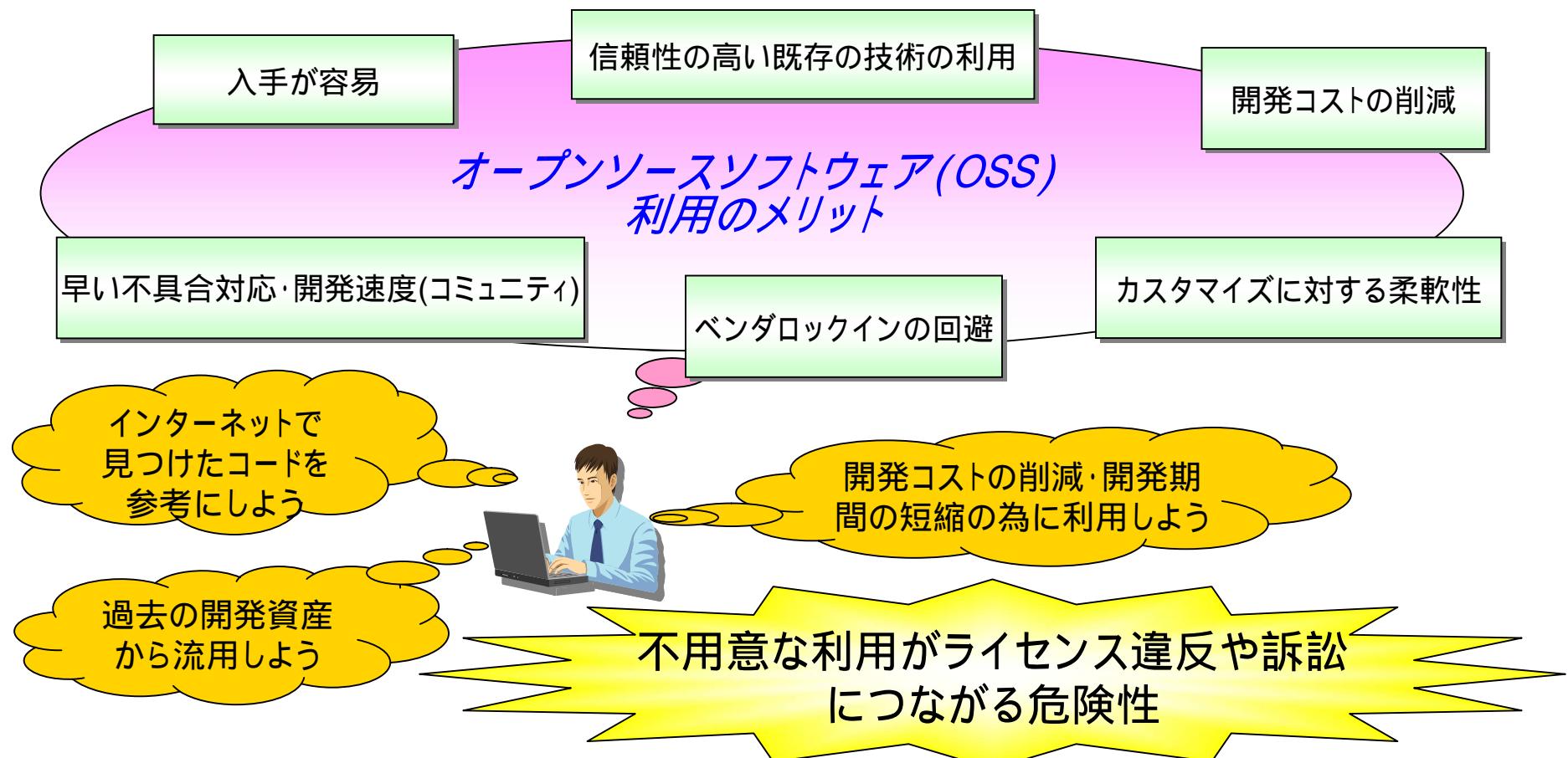


1. 背景
2. 機能・作業フロー
3. 製品・サービス体系

# 1. 背景

# OSS利用のメリットと注意点

- 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

## 過去訴訟で実際に課された条件

和解金（金額は非公開）

OSSライセンスコンプライアンス責任者の設置

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。

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 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…

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！

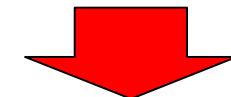
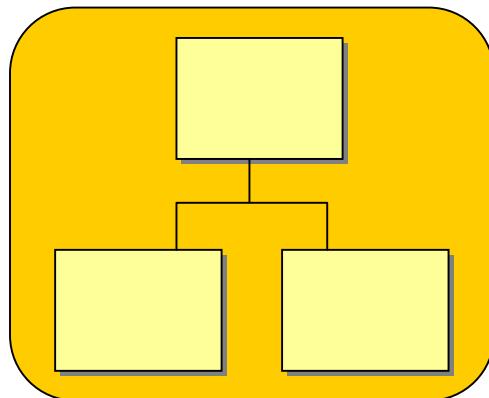
対象となった製品・事業規模によってはこれらの代償は計り知れず、  
事業や会社そのものの存続に関わる事態にもなりかねません。

# ライセンス違反を起こさないために

- ◆ 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

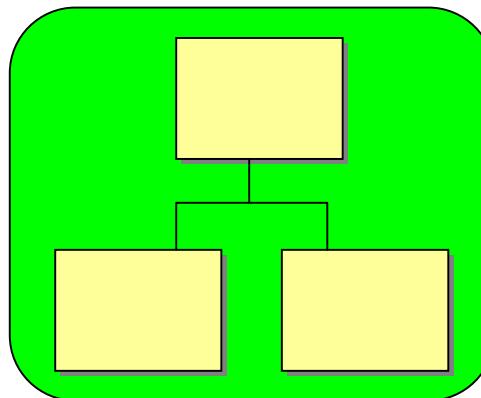
企画・設計段階での  
OSSポリシー策定

商用ライセンス



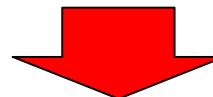
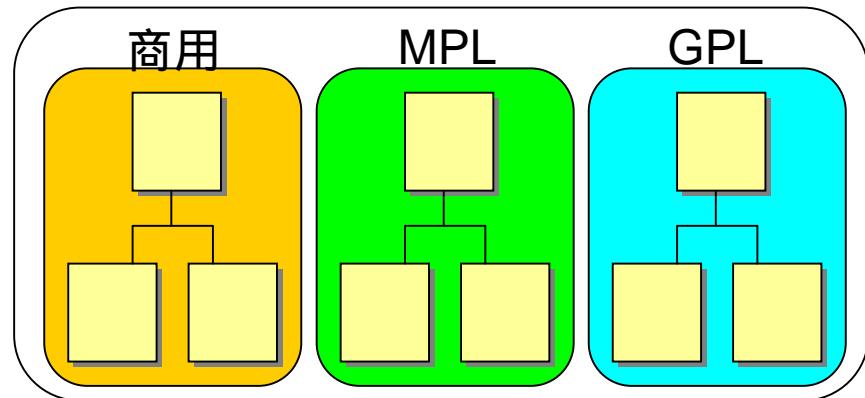
再頒布不可

単一OSSライセンス



再頒布可

複数ライセンス



再頒布不可



再頒布可

# 「思わぬ流用」はなぜ起きるのか？

## 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

- ✓ 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

なぜ?  
開発標準・品質基準など  
の統制が行き届きにくい

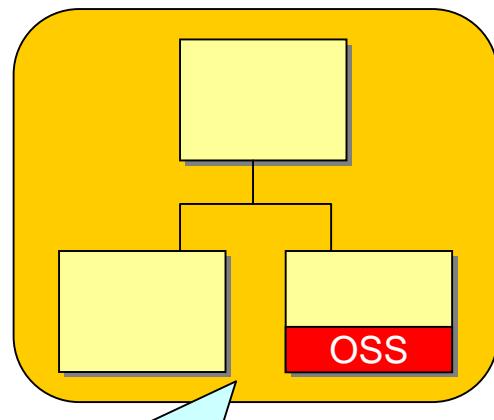


# ライセンス違反を起こさないために

- ◆ 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

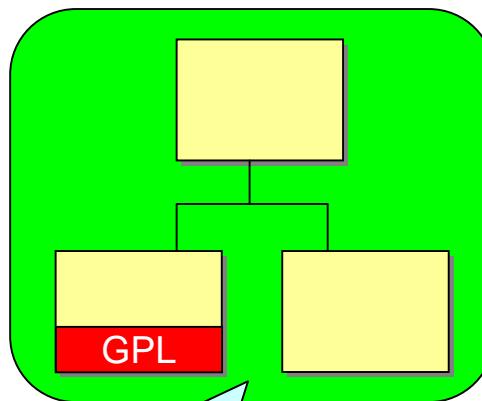
策定したOSSポリシーと  
実装が一致していることを確認

商用ライセンス



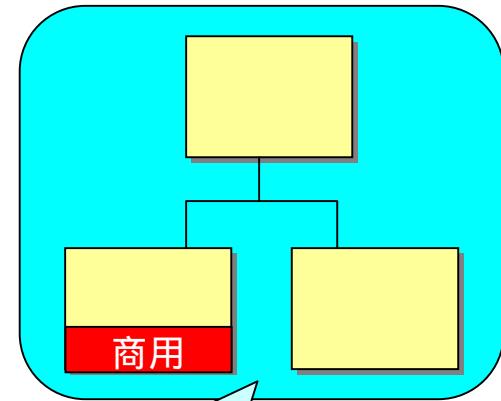
本当に  
商用ライセンス？

MPLライセンス



本当に  
MPLライセンス？

GPLライセンス



本当に  
GPLライセンス？

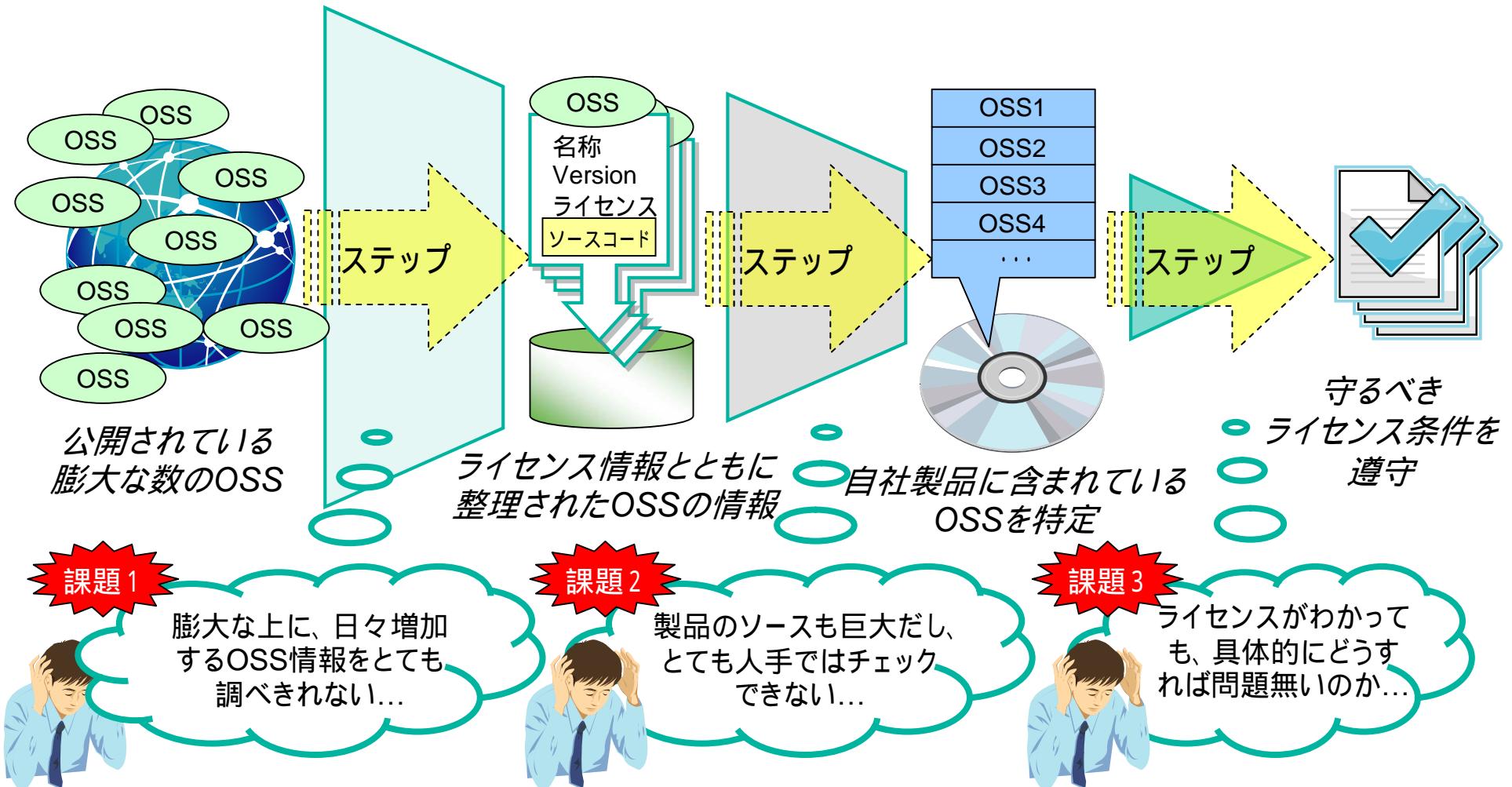
そのためには…

全ソースコードの機械的・網羅的な検査が必須



# 課題は何でしょうか？

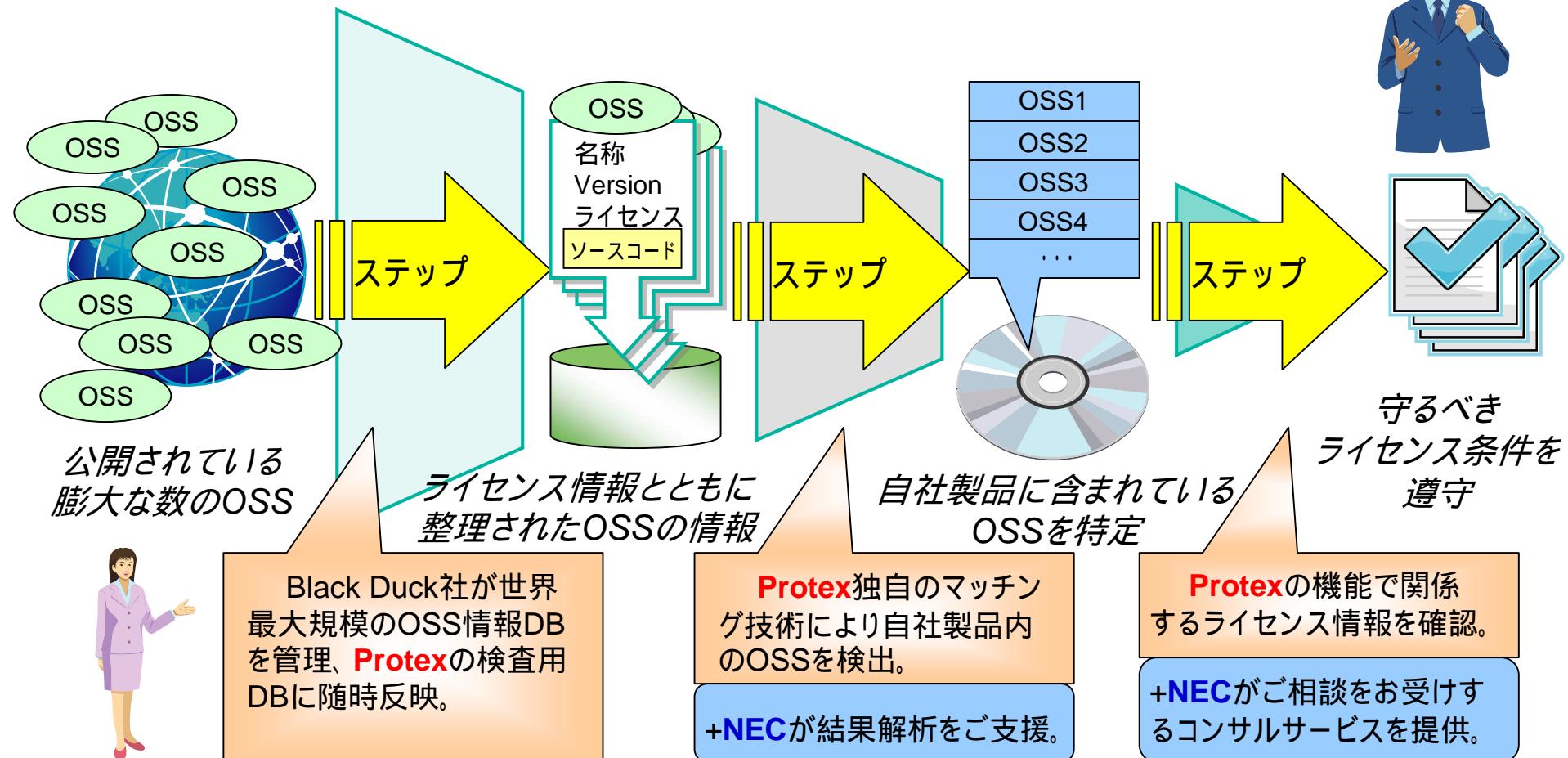
検査のために必要な各ステップから考えてみましょう。



# 私達がお手伝いします！

「**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。



## 2. 機能・作業フロー

# 機能概要

## OSS情報ナレッジベース

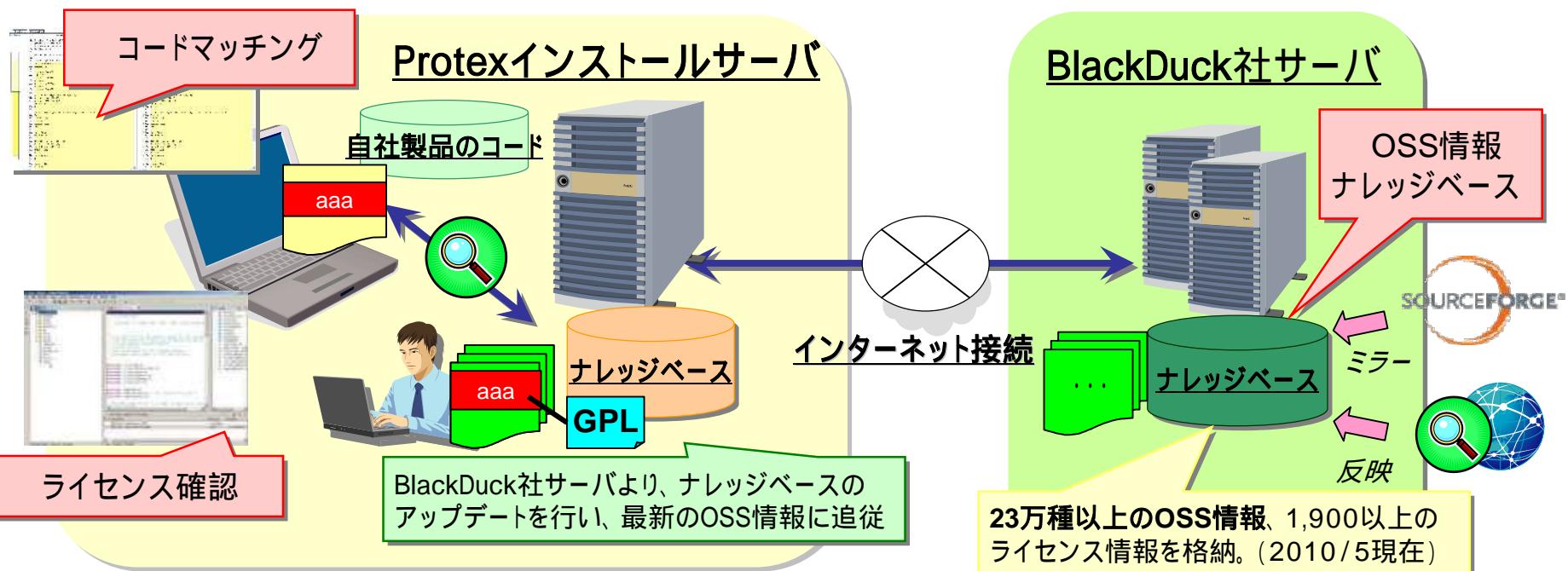
著名なOSSリポジトリサイトをミラー、その他ネット上のOSS情報を日々チェックし反映。

## 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。

## 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。



# Analysis結果からわかること

Black Duck Pro

My Protex      Manage

Current Project: Tutorial\_Files

Project Status: 388 / 0 0 0 0 0 6

388個のファイルでOSSとの一致/類似を検出

Show: Pending Identification - ALL

New Filter... Expand Collapse

Only Show Matches

- + src\_pgsl (23)
- + tools (6)
  - bftest.c
  - clean-sat.c
  - fileone.c
  - filetwo.c
  - gpgsplit.c
  - mk-tdata.c
  - mpicalc.c
  - shmtest.c
  - blowfish.c
  - openvpn.exe
  - samplefile1.h
  - samplefile2.c
  - samplefile2.c.org

Server: Server Version: 5.1.1

Bill of Materials    Code Matches    Searches    Dependencies

File: /Tutorial\_Files-20100519/tools/gpgsplit.c

Search: Go Clear

Show: Precision

| ID | Approved | Component Type | Component Name | Version | Release Date | Usage | Status          | Matched File                                    | Line | Lines |
|----|----------|----------------|----------------|---------|--------------|-------|-----------------|-------------------------------------------------|------|-------|
|    |          | GnuPG          | 1.2.4          | GPL 3.0 | 2003-12-23   | File  | Precision Match | gnupg-1.2.4.tar.gz/gnupg-1.2.4/tools/gpgsplit.c |      |       |

[First] < Prev | Next > [Last]

(print) Your File: gpgsplit.c

Matched File: gpgsplit.c

1. /\* gp...  
 2. \* Co...  
 3. \*  
 4. \* Th...  
 5. \*  
 6. \* GnuPG is free software; you can  
 7. \* it under the terms of the GNU G  
 8. \* the Free Software Foundation:  
 6. \* GnuPG is free so  
 7. \* it under the ter

検出されたOSSのプロジェクト名とライセンス

OSSのファイル100%と一致

太字のファイルで検出

# Protexをお勧めする3つの理由



強力なOSS情報ナレッジベース



高精度のマッチング機能



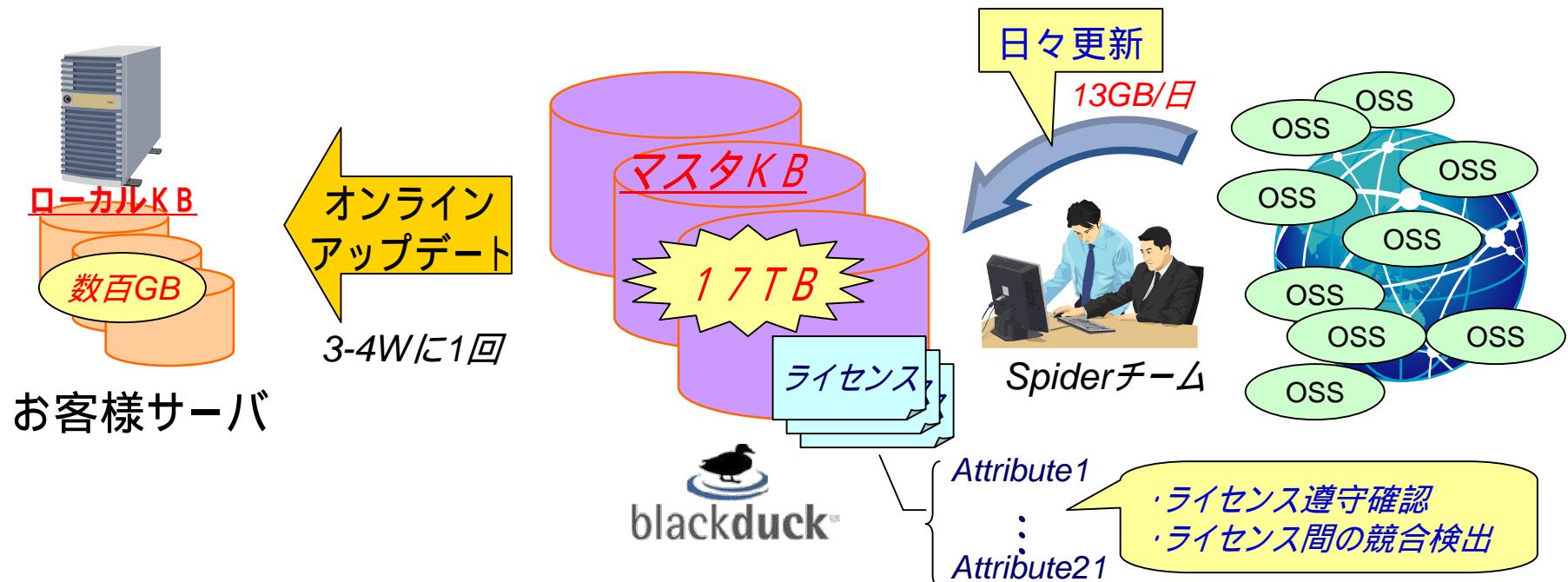
多様なカスタマイズを可能にする拡張機能

# 特長 強力なOSS情報ナレッジベース

## ■ 世界最大規模のOSS・ライセンス情報DB

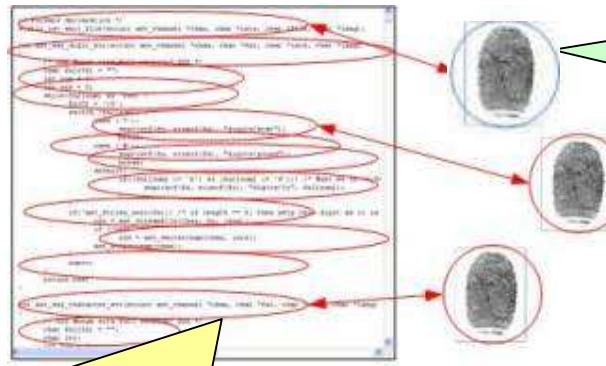
( ) 2010年5月現在 23万種以上のOSS、1,900以上のライセンス情報を格納。  
総データサイズ17TB。平均13GB/日で新規情報を追加。

- 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



# 特長 高精度のマッチング機能

- 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



Code  
Print

コード断片レベルで照合し  
類似箇所を発見



一致・類似箇所はハイライト表示

# 特長 多様なカスタマイズを可能にする拡張機能

## ■ カスタムナレッジベース

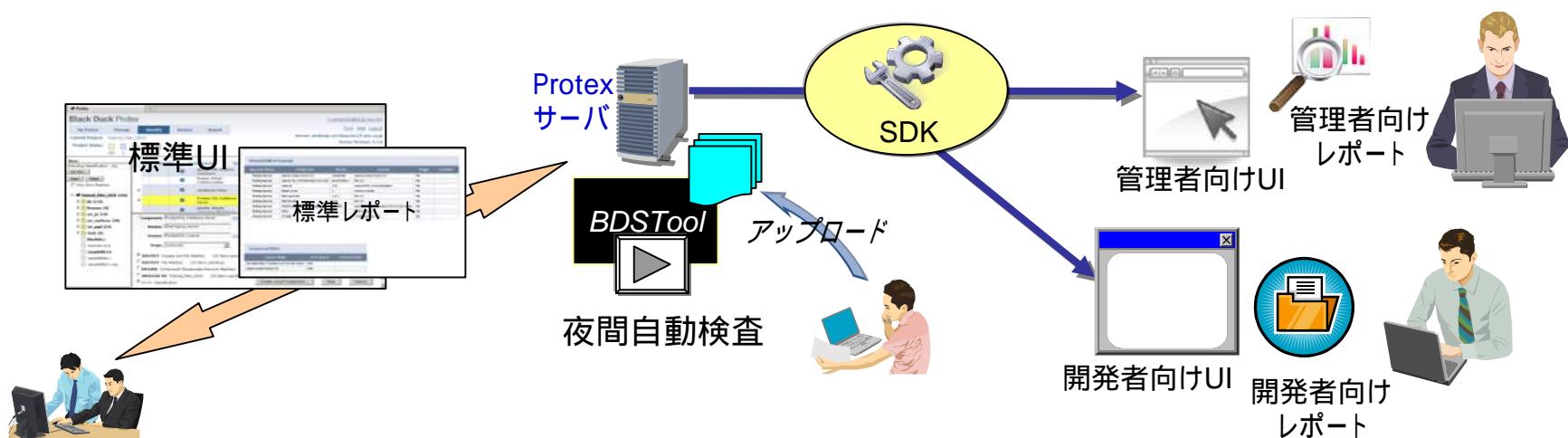
- ✓ ユーザ独自コードやライセンス定義をナレッジベースに追加登録

## ■ コマンドラインインターフェース (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)

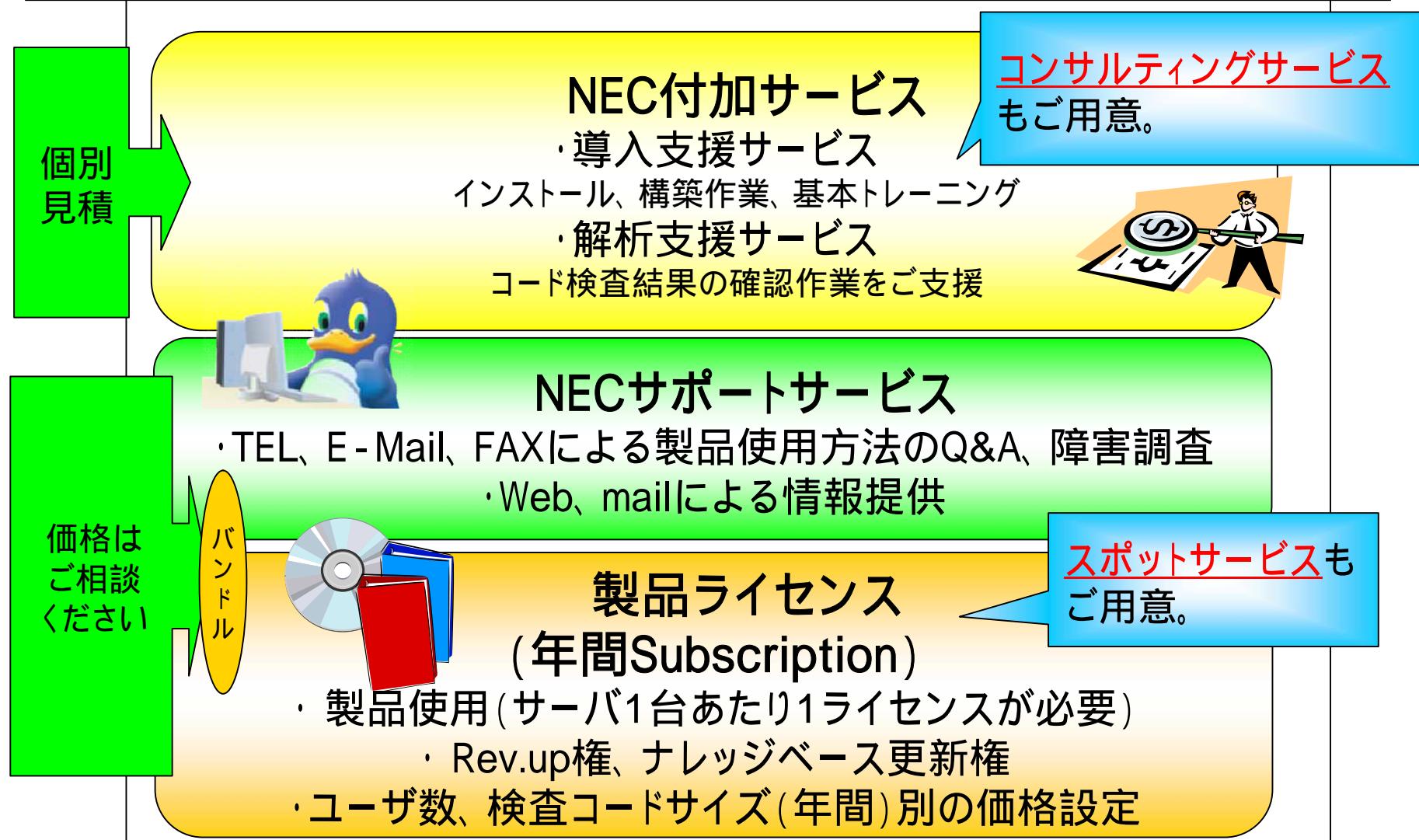
- ✓ Protexの各機能を呼び出すAPI群
- ✓ Java、C#、Perl、Pythonで利用可能
- ✓ カスタムUI・カスタムレポートなど柔軟な実装を実現



### 3. 製品・サービス体系

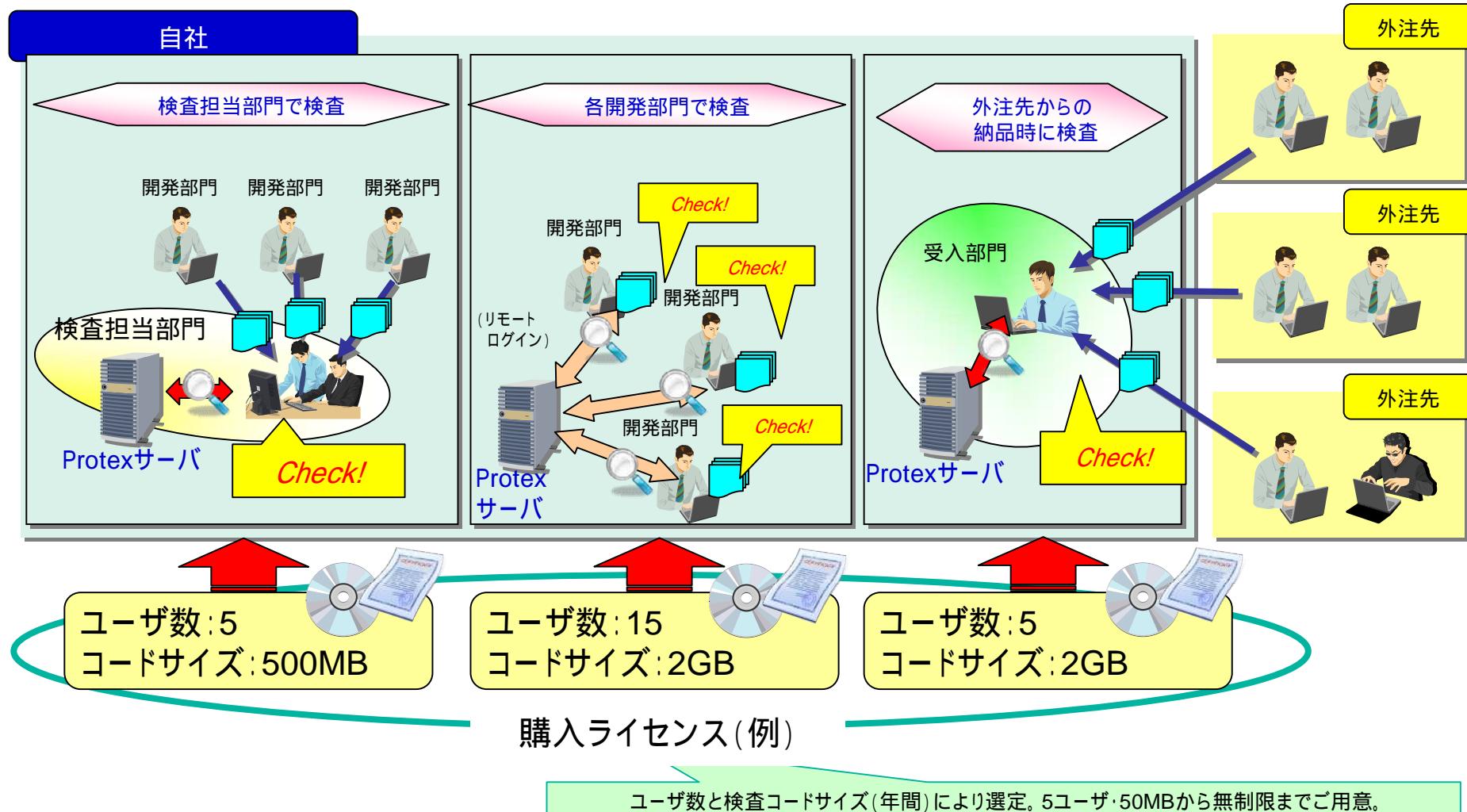
# 製品・サービス体系

➤ 製品ライセンス、サポートサービス、付加サービスで構成



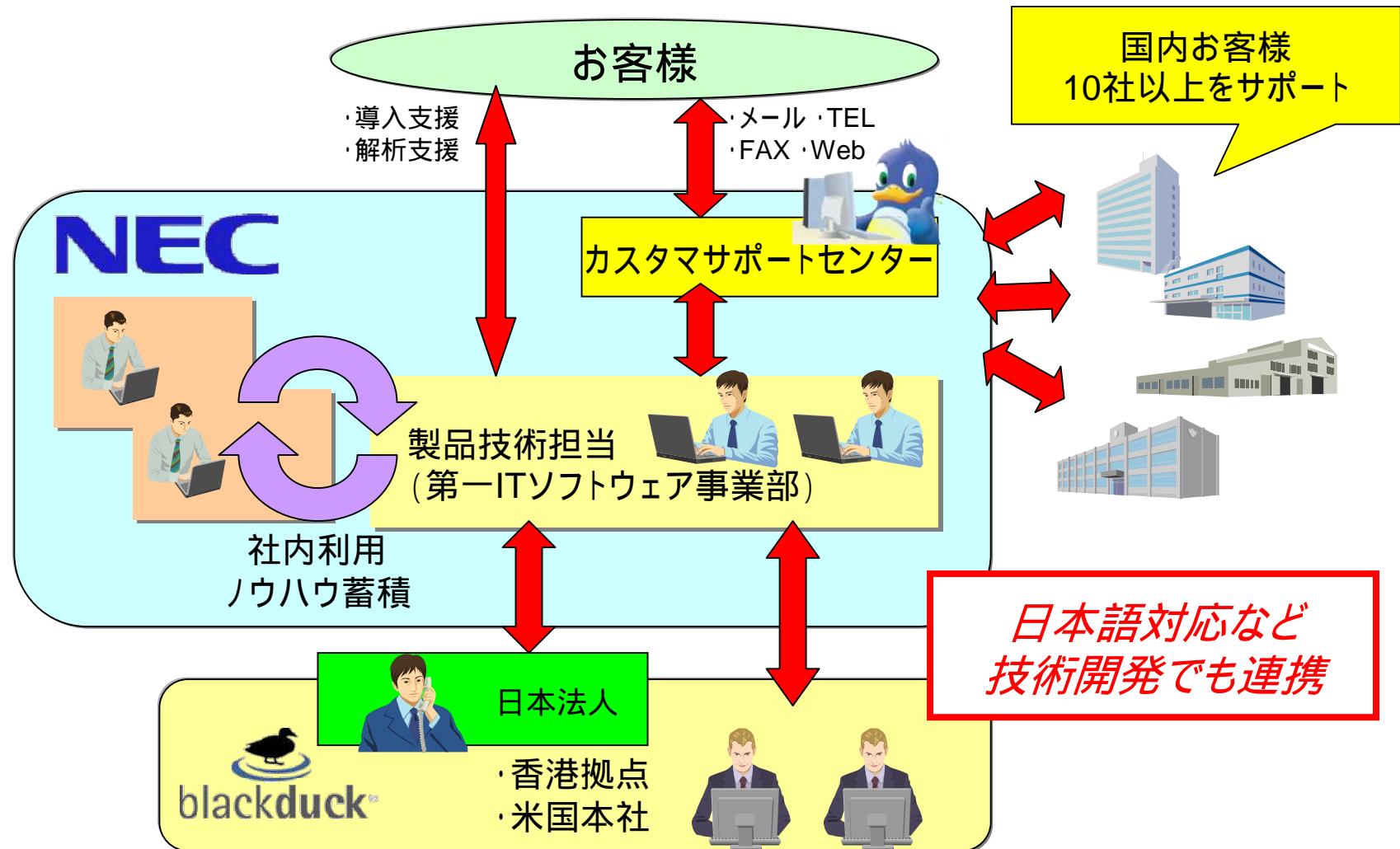
# 導入パターン

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。



# 国内サポート体制

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



# 導入支援資料「利用ガイド」(NEC作成)

**ダウンロード**

1. Protexサーバにログインし、Protexクライアントモジュールをダウンロード

- URL: <http://<Protexサーバ名 or IPアドレス>>
- 各自のユーザーIDアカウントでログイン
- ログイン後にTools → Protex client software → Download(window 60MB)と移動してモジュールをダウンロード

**インストール**

2. OSS検出ファイルの確認をする

- Only Show Matchesを選択
- Expand Allを選択
- OSS検出ファイルのみが表示されます。

**起動**

3. Reportフェースを選択

①Reportタイトルを入力  
レポートタイトルはデフォルトでテンプレート名となります。必要に応じてオーバーライドを変更することも可能です。

②項目の選択  
必要な項目は自動で選択されます。追加項目を選びたい場合はP30を参照下さい。

**プロジェクト作成**

CASE1:100%自製物件で、OSS検出無しの場合のレポート例

- Total Open Source  
- OSSとしてIdentifyしたファイルの割合が0%であれば検出OSSは無しといいます。

- Total Proprietary  
- 自製コードの割合。

- Total Unknown  
- OSSを検出したがIdentifyすることができない場合

**スキャンの実行**

CASE3:OSSが検出されLicense Conflictも発生した場合のレポート

- OSSを検出したがIdentifyすることができない場合

**判定作業の実施**

①Declared License Conflict  
利用しているOSSのライセンスとプロジェクトの既存ライセンスとの間で両方同時に付箋せないライセンス異界が存在していることを表します。  
例) 商用ライセンスでの表示「ソース非開示」と、GPLでの表示「ソース開示」。

②Component License Conflict  
利用しているOSSのライセンス間で、両方同時に付箋せないライセンス異界が存在していることを表します。  
例) GPLの表示「既存物へのGPL適用」と、MPLの表示「既存物へのMPL適用」。

確認方法

1. レポート「Bill of Materials」にて、項目「License Conflict」の値が「Declared Licence Conflict」及び「Component Licence Conflict」になっているOSSを確認し、その度数をチェック。  
- 「Declared Licence Conflict」のOSSが多く、「Component Licence Conflict」の少ない場合  
⇒ Component Licence Conflictの表示が「既存物へのライセンス異界」、License Conflictの表示は「既存物」となります。  
- 「Declared Licence Conflict」のOSSがある場合  
⇒ 2次元へ整理してください。

例: Bill of Materials

| Approved Status  | License Conflict           | Component |
|------------------|----------------------------|-----------|
| Pending Approval | Declared license conflict  | Project A |
| Pending Approval | Component license conflict | Project B |

2. Component license conflictの状況を確認するには、該当する「Bill of Materials」を確認すればOKです。

# 無料体験のご案内

お試し版レポート、評価ライセンスの2種類をご用意。

## お試し版レポート

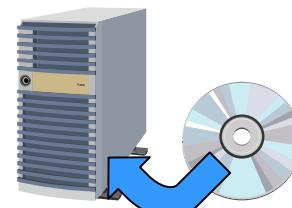
- お客様のソースコード(最大25MB)をお預かりし、スキャン結果をお返します。
- 正規製品の出力との差分はありません。
- 機材のご準備は不要です。



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

## 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！

# ソースコード第三者検証サービス

- 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

開発ソースコード

複数の静的検証ツール群

ツール出力結果  
(大量なメッセージ)

検出問題を統合



開発者のスクリーニング  
は大変な負荷

専任者の精査により重要  
問題の見落とし極小



➤ 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](mailto: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

**NEC**