

「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

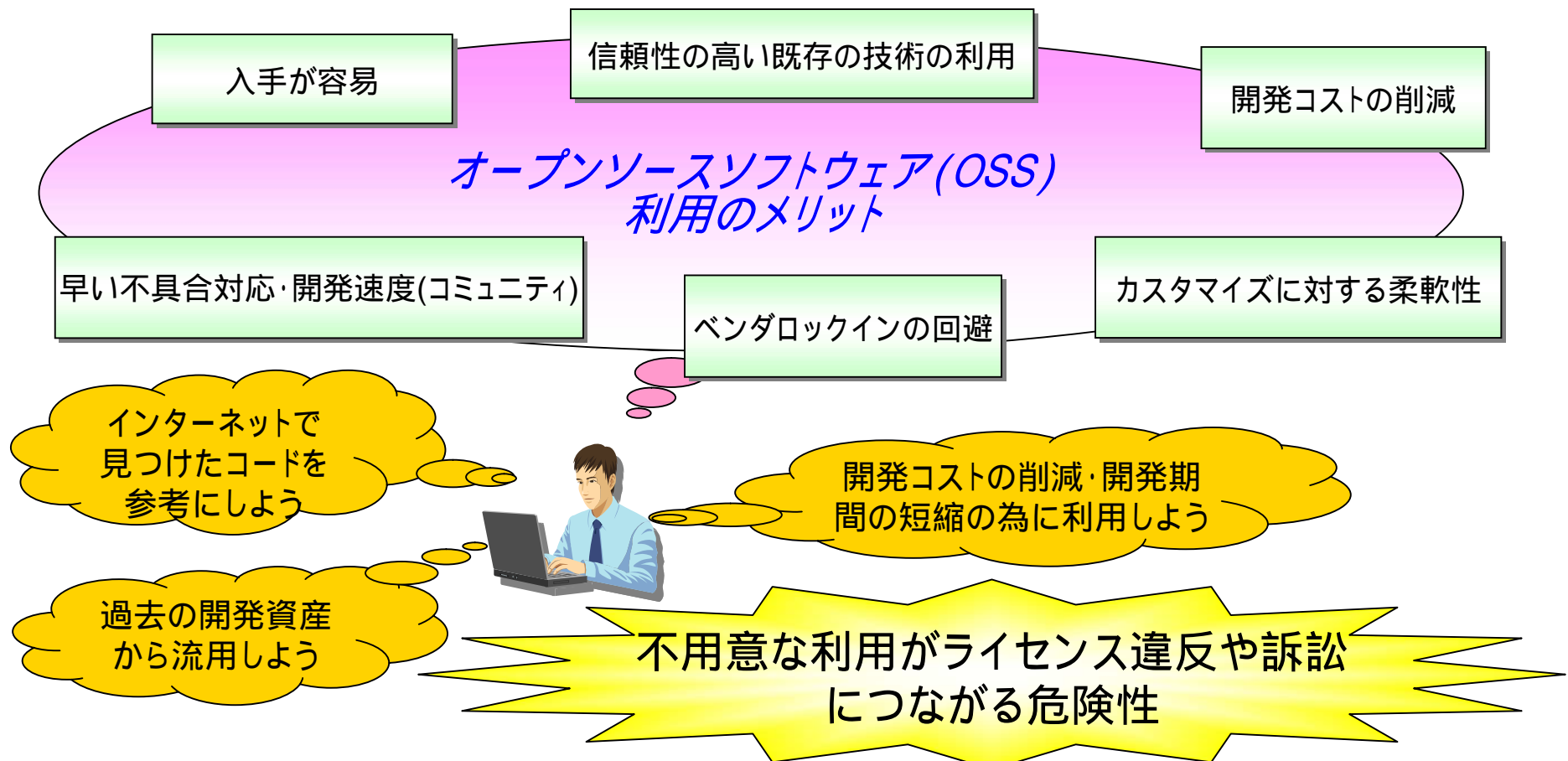


1. 背景
2. 機能・作業フロー
3. 製品・サービス体系

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！**

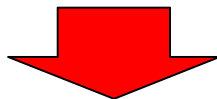
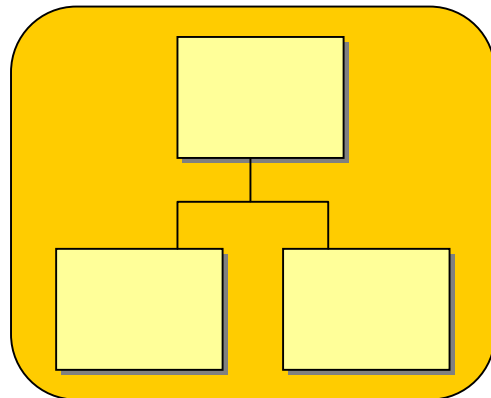
対象となった製品・事業規模によってはこれらの代償は計り知れず、
事業や会社そのものの存続に関わる事態にもなりかねません。

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

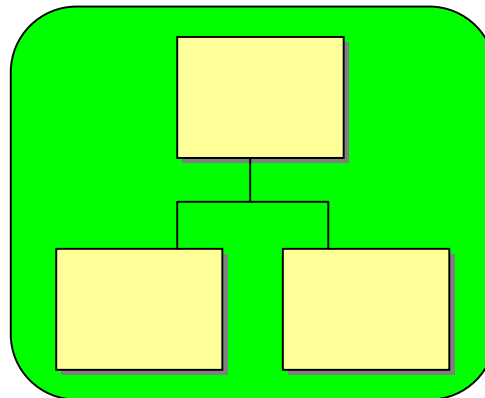
企画・設計段階での
OSSポリシー策定

商用ライセンス



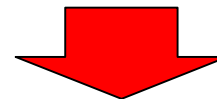
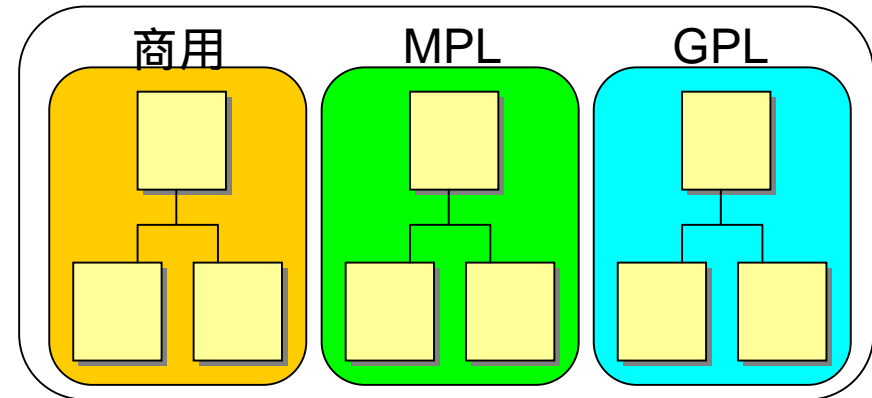
再頒布不可

単一OSSライセンス

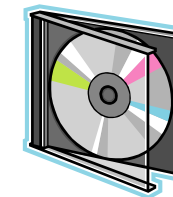
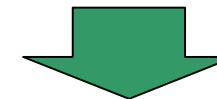


再頒布可

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を使っていないいつも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

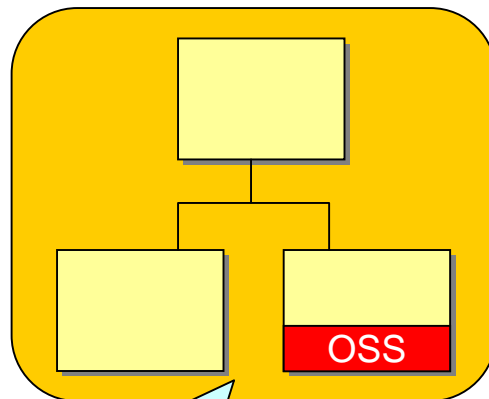
ライセンス違反を起こさないために

- ◆ 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

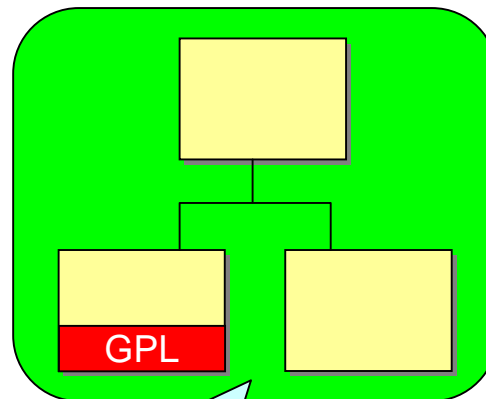
策定したOSSポリシーと
実装が一致していることを確認

商用ライセンス



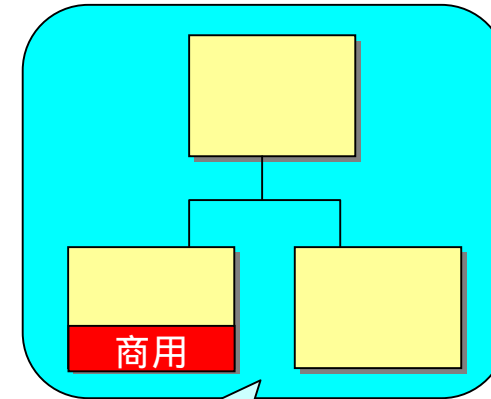
本当に
商用ライセンス？

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？

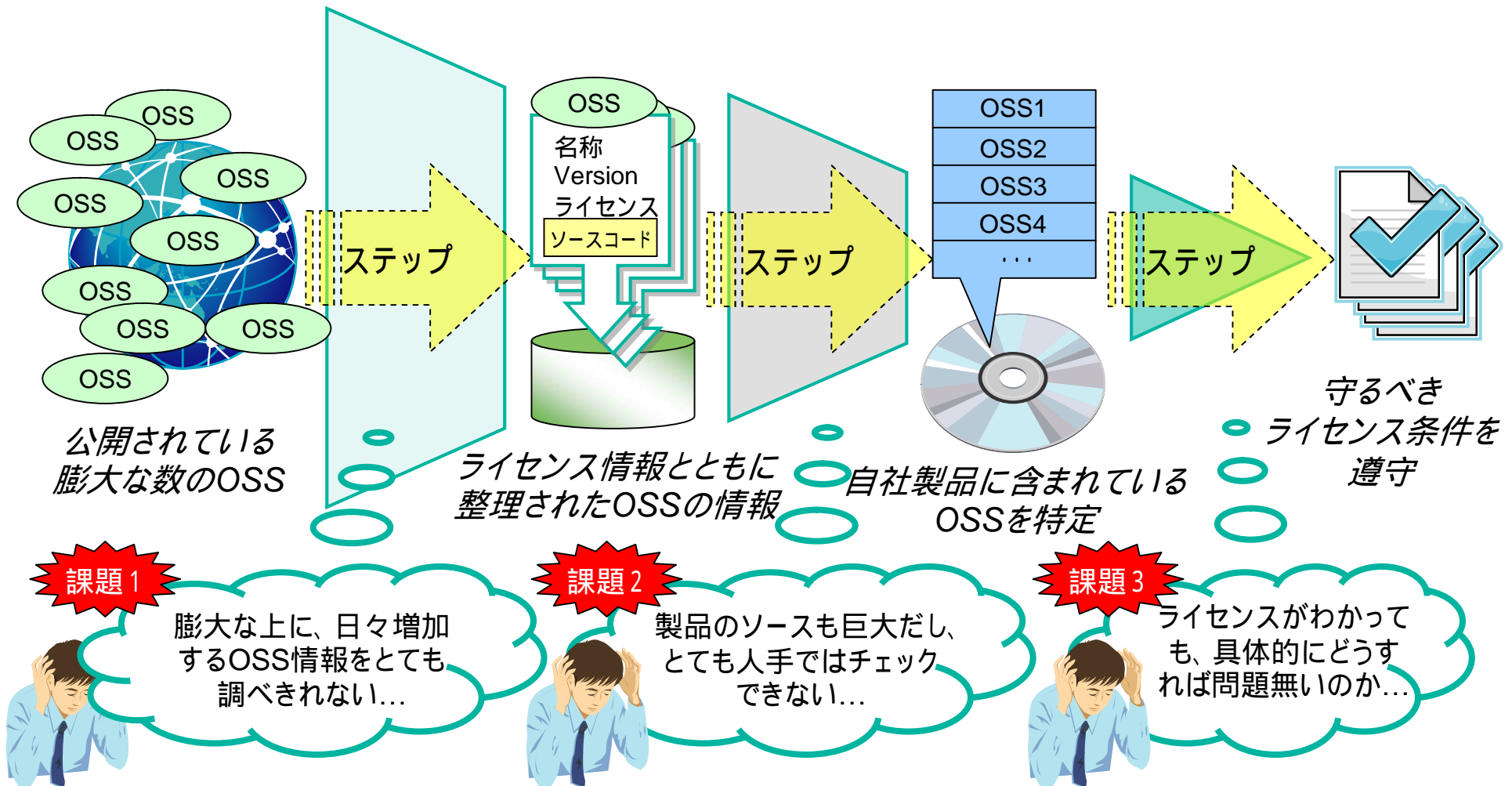
そのためには・・・

全ソースコードの機械的・網羅的な検査が必須



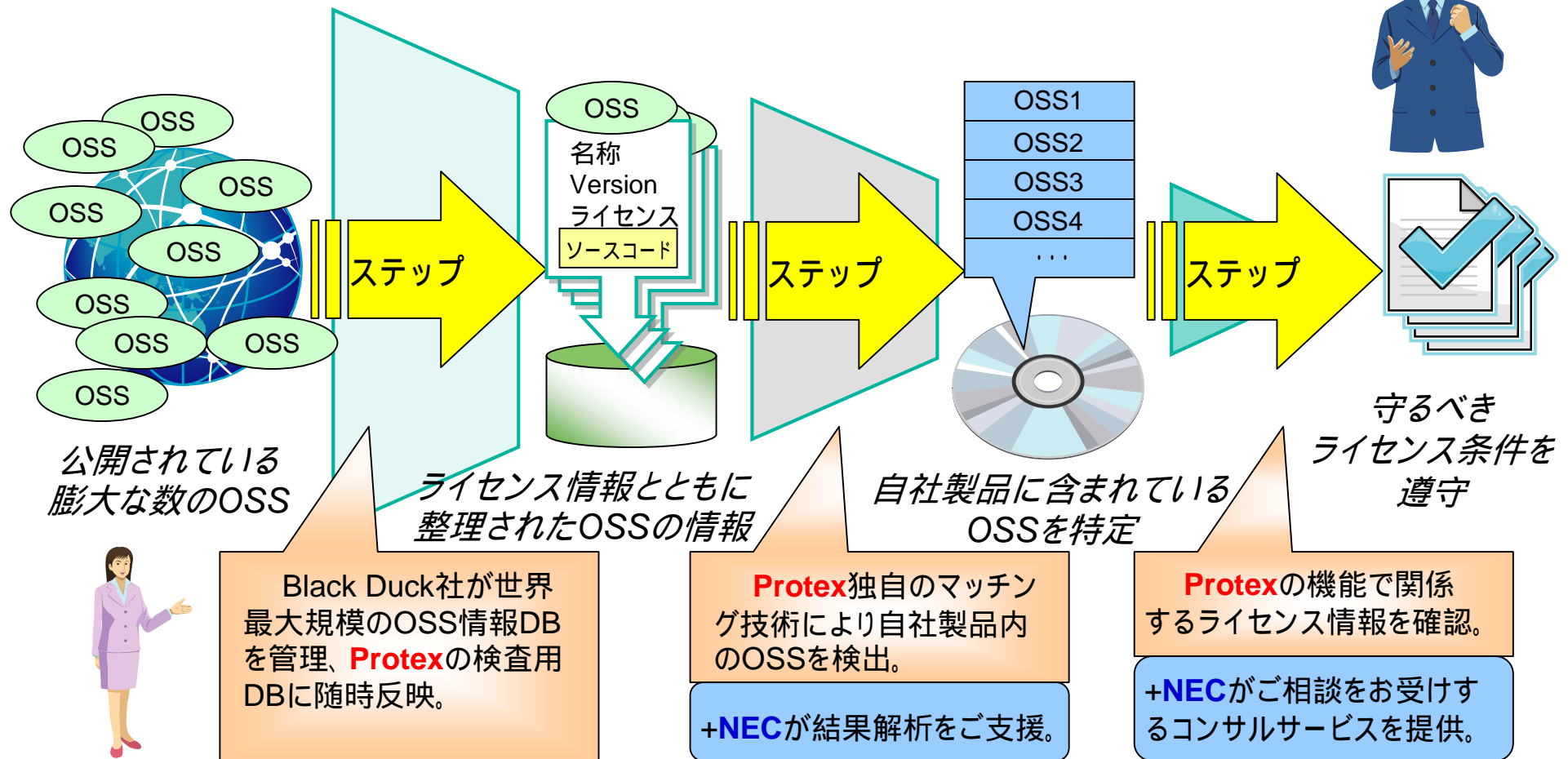
課題は何でしょうか？

■ 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

OSS情報ナレッジベース

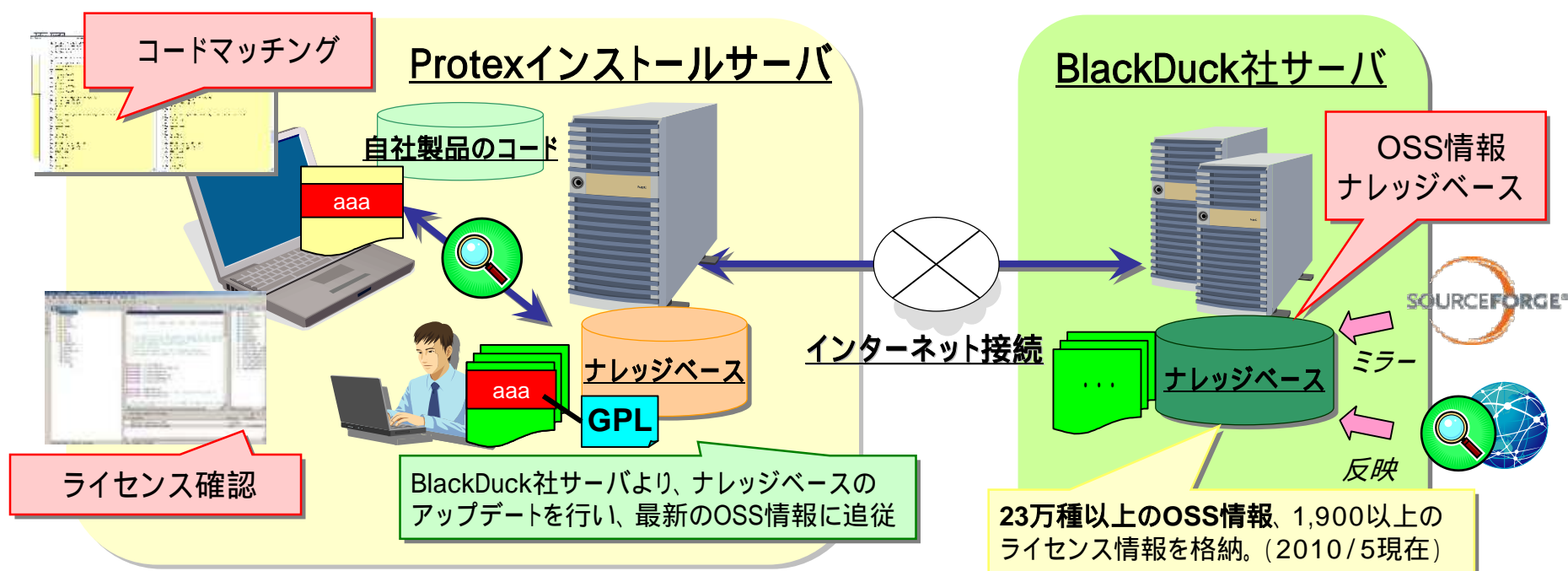
著名なOSSリポジトリサイトをミラー、その他ネット上のOSS情報を日々チェックし反映。

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

388個のファイルでOSSとの一致/類似を検出

388 0 0 0 0 0 6

Current Project: Tutorial_Files

Project Status: ■ ■ ■ ■ ■ ■

Tools Help Logout

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

1 Component

ID	Approved	Component Type	Component Name	Version	License	Release Date	Usage	Status	Match %	Matched File	Line #	Lines
		Library	GnuPG	1.2.4	GPL 3.0	2003-12-23	File	Precision Match	100	gpgsplit.c		

Connect All Matches in New Window

(print) Your File: gpgsplit.c Matched File: gpgsplit.c

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

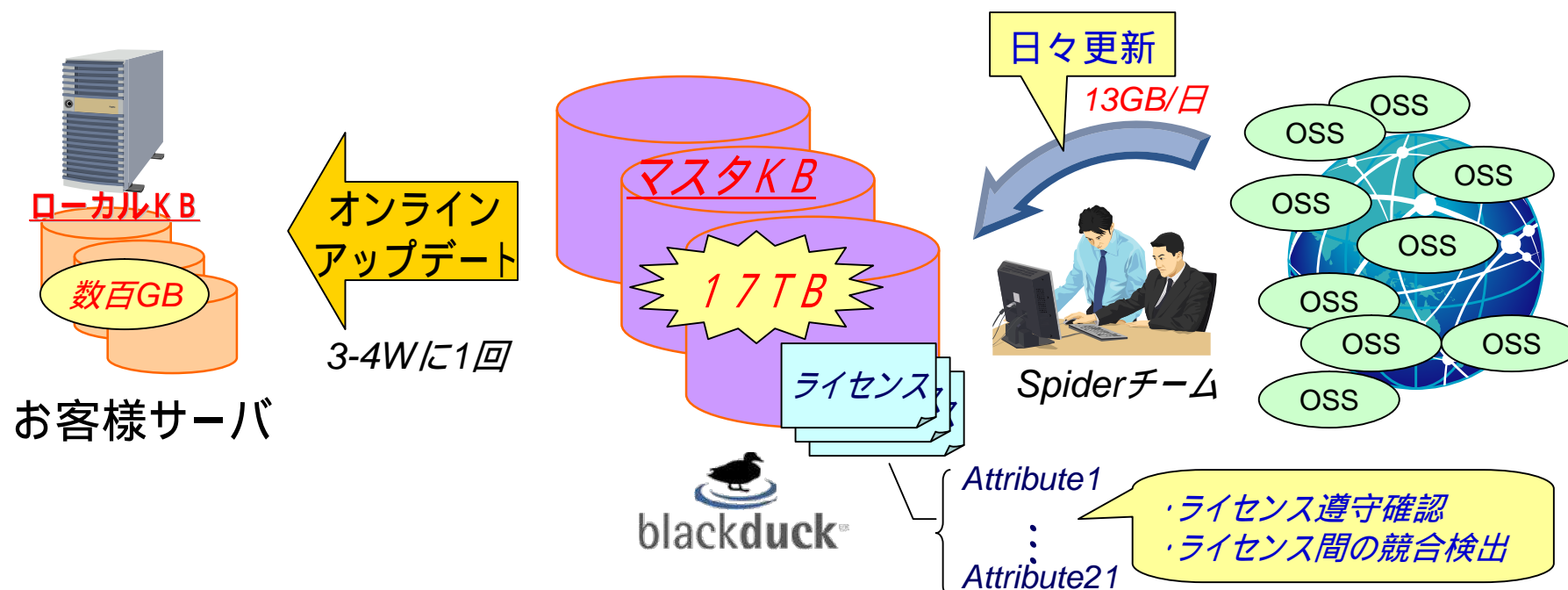
特長 強力なOSS情報ナレッジベース

■ 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。

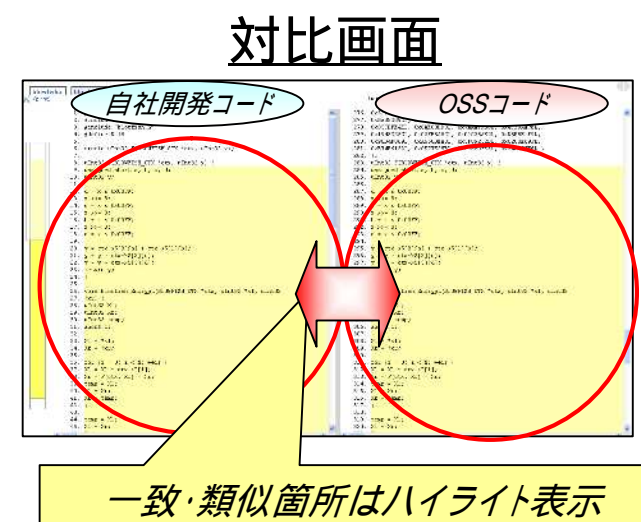
■ ソースコードだけでなくバイナリ(ライブラリ、アイコン等)も格納

■ 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



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

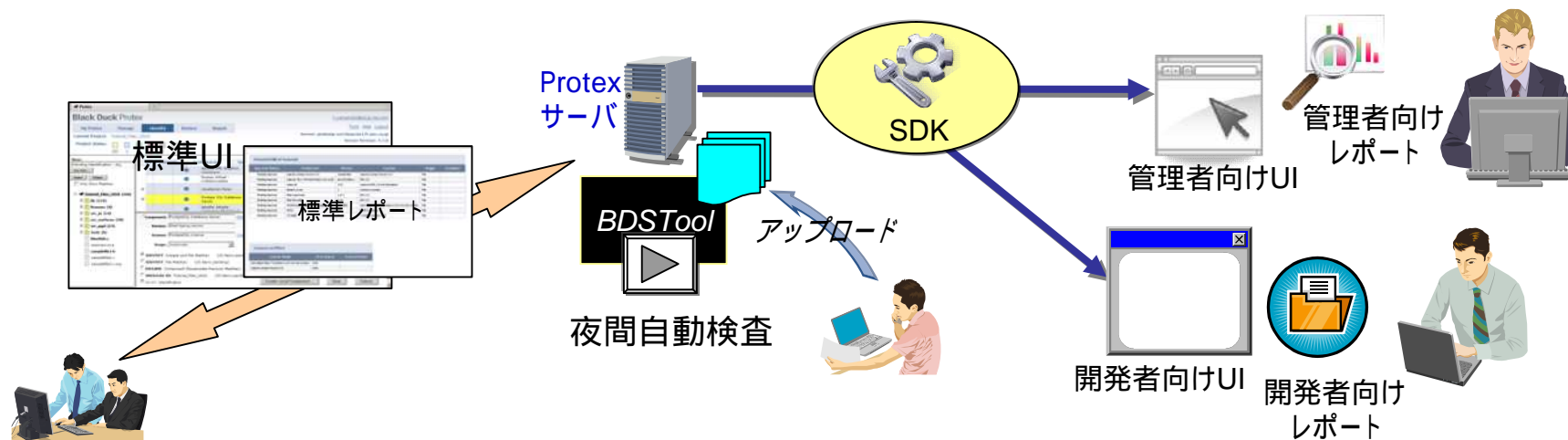
- ✓ ユーザ独自コードやライセンス定義をナレッジベースに追加登録

■ 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

個別
見積

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。

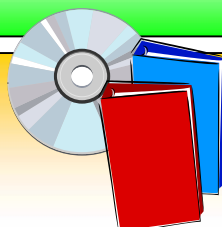


NECサポートサービス

- ・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



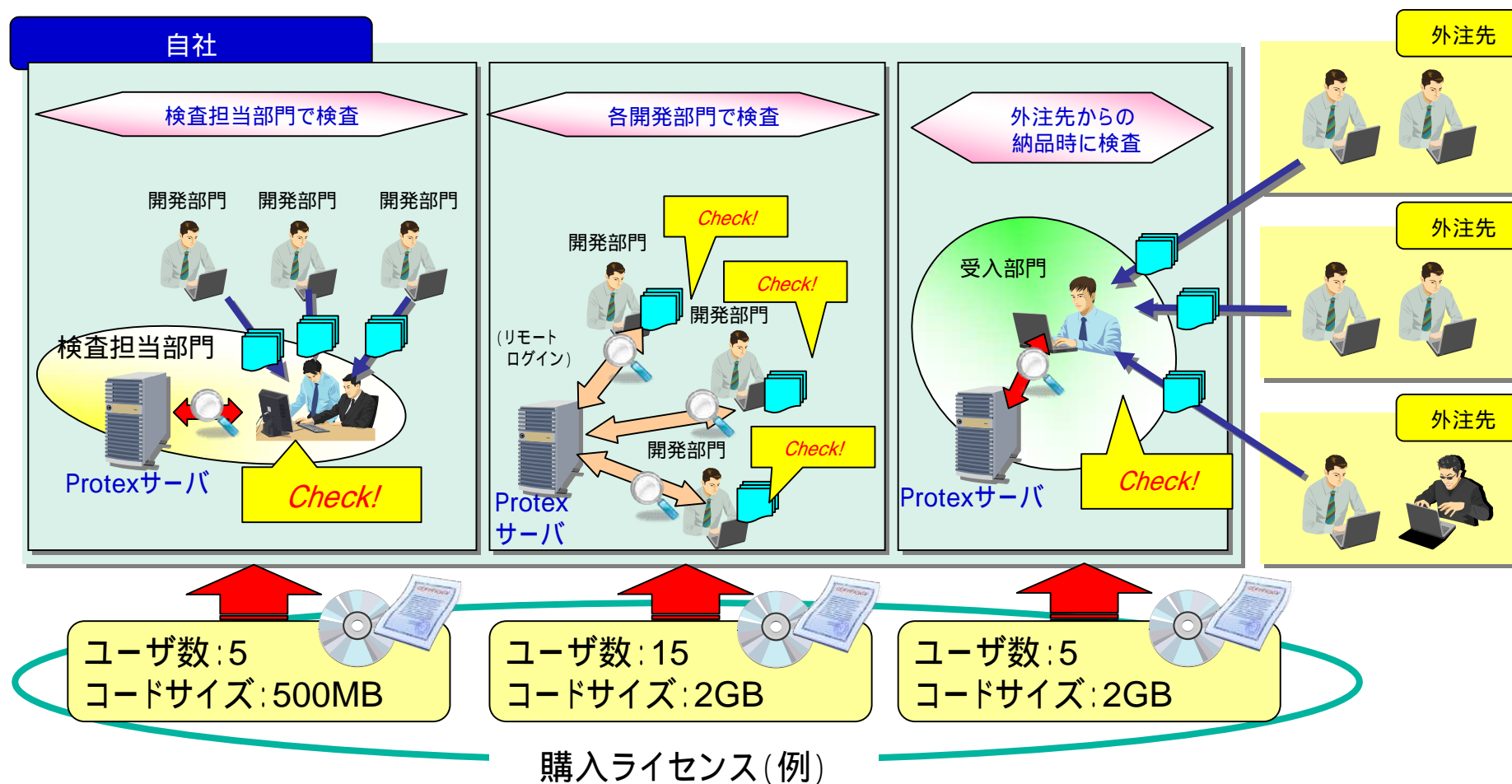
製品ライセンス (年間Subscription)

- ・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

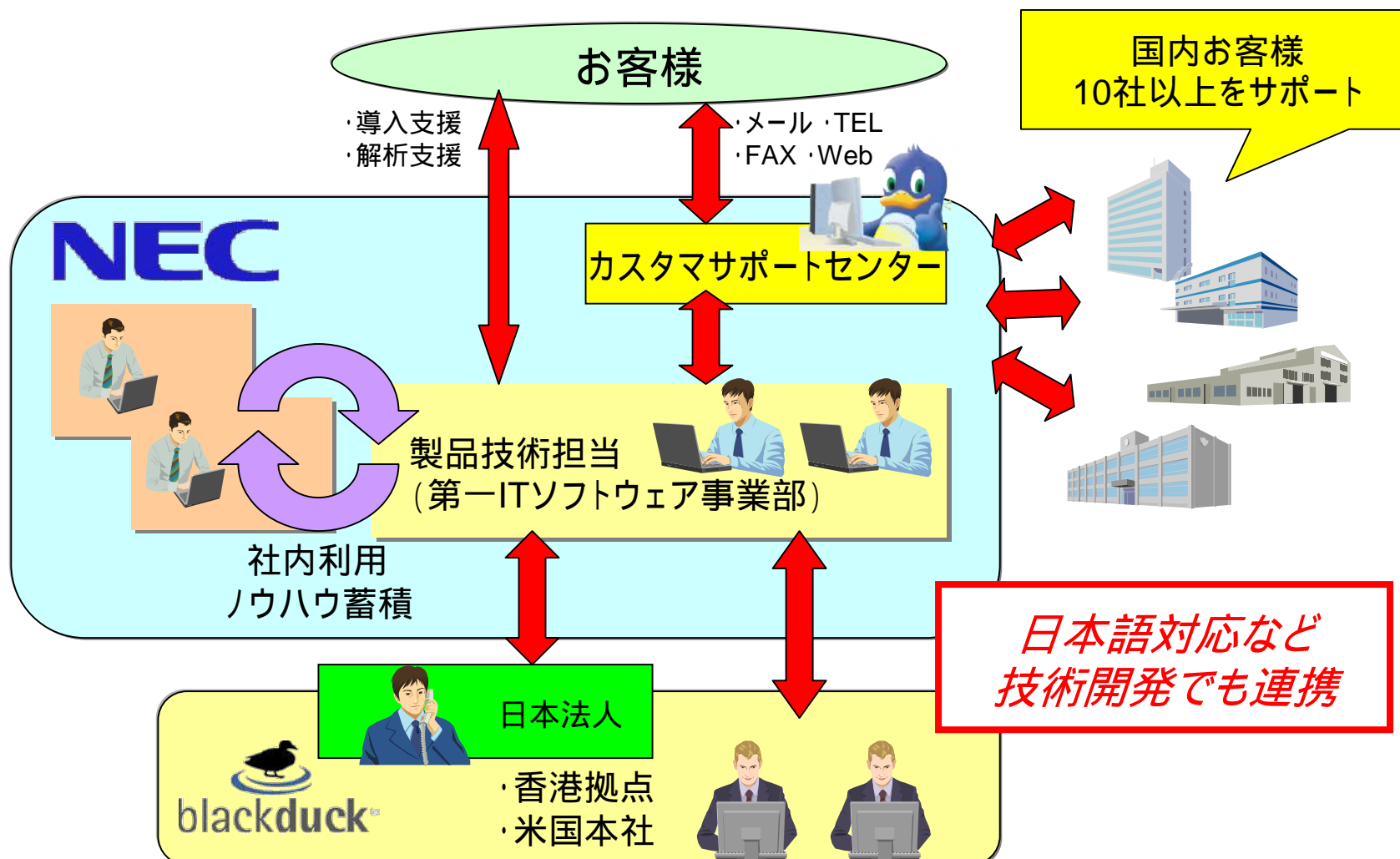
お客様の開発/品質管理体制・組織構造に応じ、様々な導入パターンが可能。



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

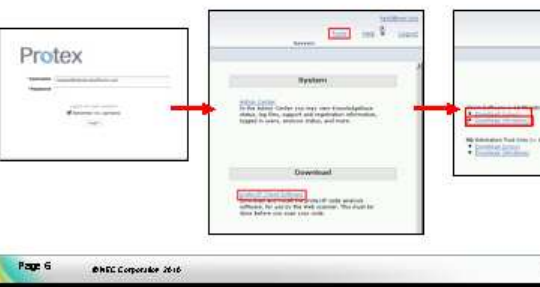
自社利用で蓄積したノウハウ、開発元Black Duck社との密連携により
日本のお客様に安心のサポートをご提供



ダウンロード インストール 起動

1. Protexサーバーにログインし、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




Page 6 ©NEC Corporation 2016

プロジェクト作成 スキャンの実行 判定作業の実施

①ステータスバーで状態を確認
Project Statusで以下のように表示されます。
OSS検出率100%であれば、**緑色の**あるOSSが検出されなかったということになります。

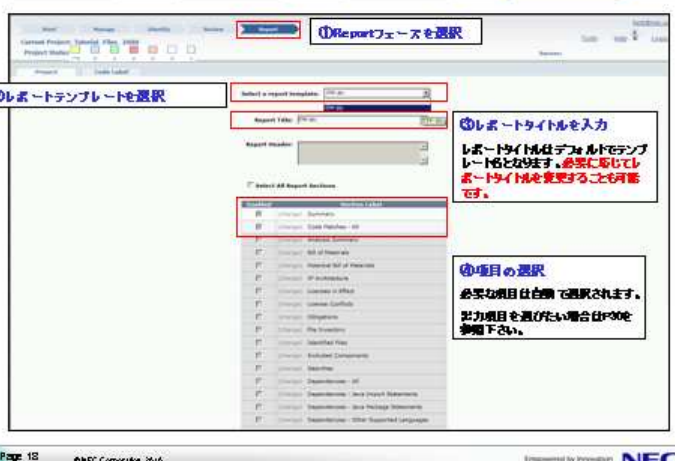
②OSS検出ファイルの検出をする
1. Only Show Matchedを選択
2. Expand Allを選択
3. OSS検出ファイルのみが表示されます。



Page 11 ©NEC Corporation 2016

プロジェクト作成 スキャンの実行 判定作業の実施 レポートの出力

①Reportフェースを選択
②レポートテンプレートを選択
③レポートタイトルを入力
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。必要に応じてレポートタイトルを変更することも可能です。
④項目の選択
必要な項目は白欄で選択されます。出力項目を選びたい場合はF000を参照下さい。



Page 12 ©NEC Corporation 2016 Empowered by Innovation NEC

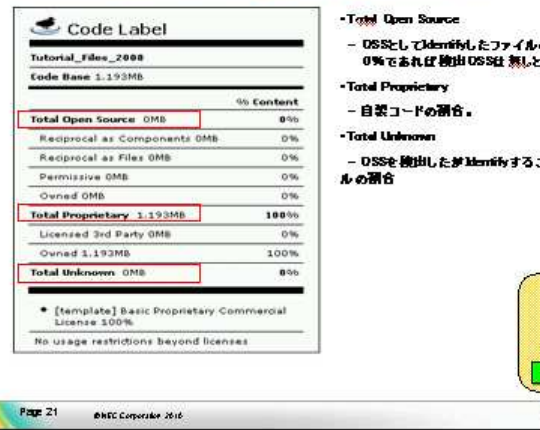
プロジェクト作成 スキャンの実行 判定作業の実施

CASE1:100%自製物件で、OSS検出無しの場合のレポート例

Code Label
Tutorial_Files_2000
Code Base: 1.193MB

	% Content
Total Open Source OMB	0%
Reciprocal as Components OMB	0%
Reciprocal as Files OMB	0%
Permissive OMB	0%
Owned OMB	0%
Total Proprietary 1.193MB	100%
Licensed 3rd Party OMB	0%
Owned 1.193MB	100%
Total Unknown OMB	0%

• Total Open Source
- OSSとしてIdentifyしたファイルの割合0%であれば検出OSSは無しといえます。
• Total Proprietary
- 自製コードの割合。
• Total Unknown
- OSSを検出したがIdentifyすることのできなかったものの割合

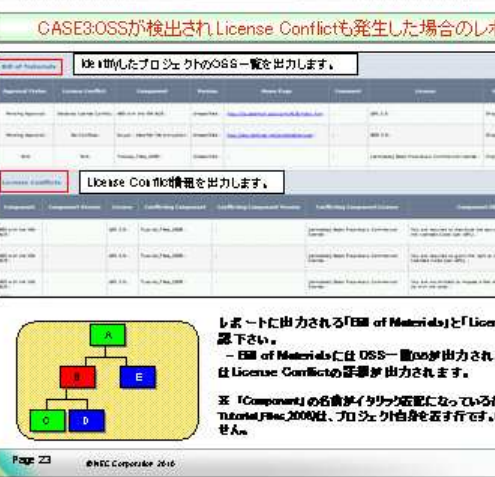


Page 21 ©NEC Corporation 2016

プロジェクト作成 スキャンの実行 判定作業の実施

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

1. 検出したプロジェクトのOSS一覧を出力します。
2. License Conflict情報を出力します。



Page 23 ©NEC Corporation 2016

CASE3補足: License Conflictの確認方法(1)

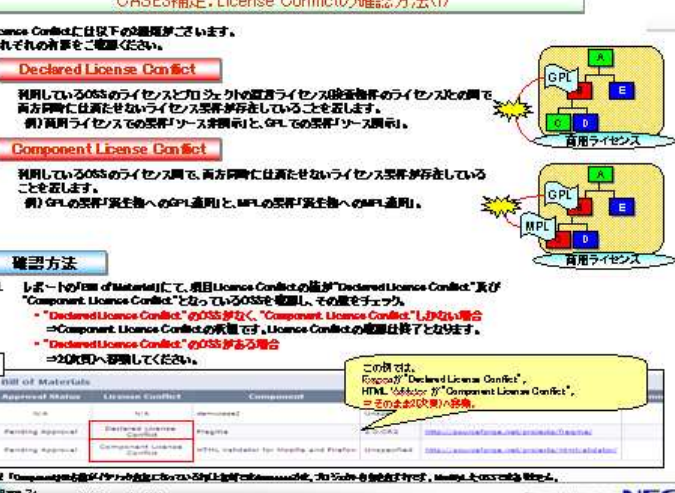
License Conflictには以下の2種類があります。それぞれの特徴をご確認ください。

Declared License Conflict
利用しているOSSのライセンスとプロジェクトの直間ライセンス/依存関係のライセンスとの間で両方同時に満たされないライセンス要件が存在していることを示します。
例) 両方ライセンスでの要件がソース非開示と、GPLでの要件がソース開示。

Component License Conflict
利用しているOSSのライセンス間で、両方同時に満たされないライセンス要件が存在していることを示します。
例) GPLの要件が派生物へのGPL適用と、MPLの要件が派生物へのMPL適用。

確認方法
1. レポートの「BOM of Materials」にて、項目License Conflictの値が"Declared License Conflict"及び"Component License Conflict"となっているOSSを確認し、その数でチェック。
- "Declared License Conflict"のOSSが無く、"Component License Conflict"しかない場合
⇒ Component License Conflictの範囲です。License Conflictの範囲は狭くなります。
- "Declared License Conflict"のOSSがある場合
⇒ 2次開発へ影響してください。

例) この図では、Reportの"Declared License Conflict", "HTML"の"Component License Conflict", 2つの2次開発へ影響。



Page 24 ©NEC Corporation 2016 Empowered by Innovation NEC

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

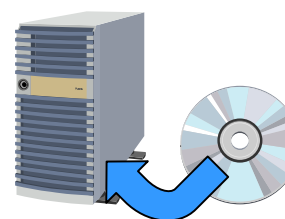
- お客様のソースコード(最大25MB)をお預かりし、スキャン結果をお返しします。
- 正規製品の出力との差分はありません。
- 機材のご準備は不要です。



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 + + / J A V A

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

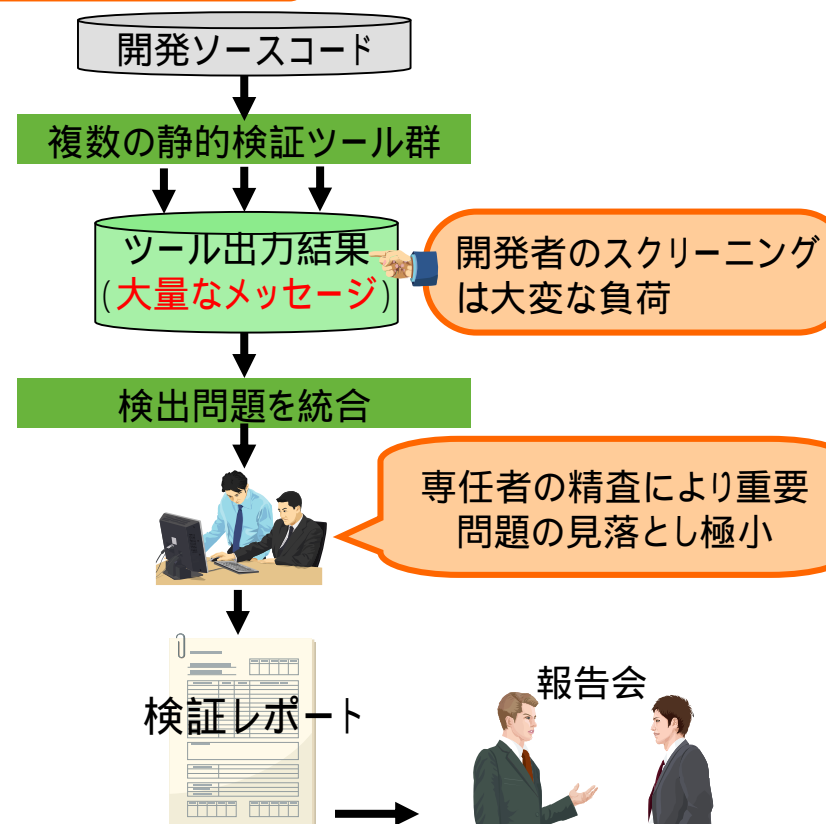
開発者に負荷をかけたくない時に

- 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



➤ 製品情報

<http://www.nec.co.jp/oss/protexip/>

➤ お問い合わせ

E-Mail: protexip-info@ossfp.jp.nec.com

(NEC 第一ITソフトウェア事業部 Protex担当)



Empowered by Innovation

NEC