ソフトウェアテストシンポジウム 2009 東京

OSSコード検出ツール「protexIP」のご紹介

(あなたの製品でOSSライセンス違反を起こさないために)

2009年1月29日
NEC OSSプラットフォーム開発本部
山本

Contents

1. 背景

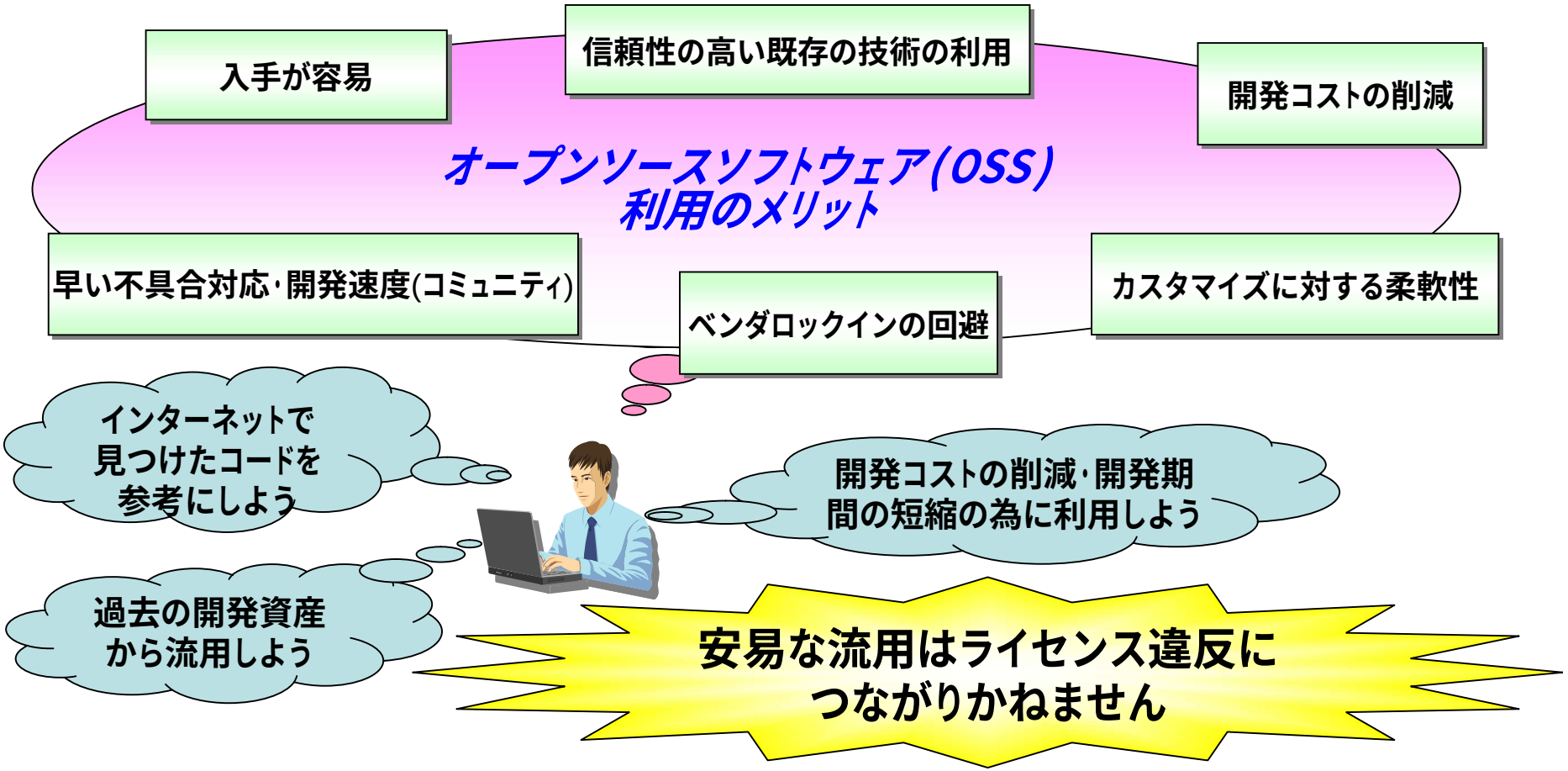
2. 特長･機能ご紹介
   - デモンストレーション

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。



OSSライセンス違反に関する事例(1)

◆ GPL(GNU Public License)違反に関する事例は、日本を含め多数存在

米:Fortinet社の事例

製品FortiGate・FortiWiFi内のSWに、GPLのコンポーネントである「initrd」等を利用。
しかしながら、ソースコードを非公開とし、暗号化技術によって「initrd」等の利用を隠匿。

initrdの開発者であるHarald Welte氏が違反を指摘するが、適切な対応がなかったため、Fortinet社を提訴。
2005年4月12日、ミュンヘン地裁はFortinet社に対し、該当製品販売禁止の仮差止命令を下す。
(最終的に、Welte氏とFortinet社はGPLを遵守することで和解)

日本:ネットワーク機器メーカの事例

ネットワーク機器のファームウェアにLinuxカーネルやglibcを初めとするGPLのコンポーネントを利用。
しかしながら、ソースコードを非公開としていた。

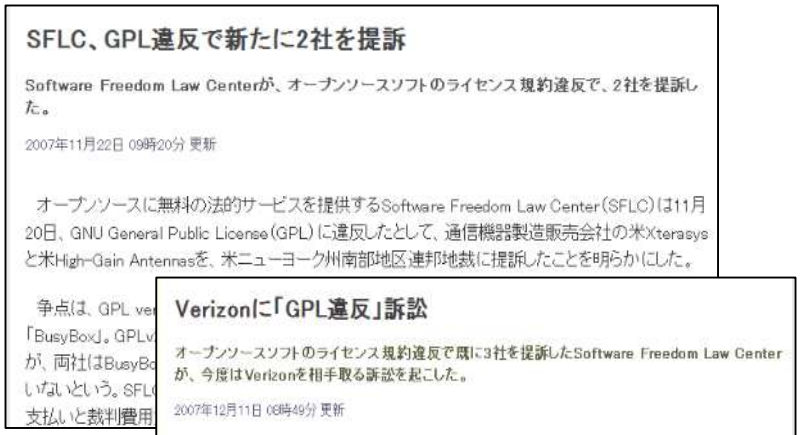
サイトからファームウェアをダウンロードした購入ユーザからGPL違反の疑いを指摘されるが、
「独自物件であり公開の必要はない」と不適切な対応を取ったため、Internet上で批判・反発が発生。
(最終的にGPLを遵守。訴訟には至らなかったが、企業イメージ低下を招いた)

OSSライセンス違反に関する事例(2)

◆「SFLC (Software Freedom Law Center)」によるGPL違反訴訟

SFLCは、OSSを法的側面から支援する非営利団体

2007年9月以降、デジタル家電メーカ・無線機器メーカに対し、「提供製品内でGPLのコンポーネントを利用しているにも拘らず、ソースコード公開義務を遵守していない」として、開発者を代表する形で立て続けに訴訟を起こしたことで注目を集めている。(一部は、「GPLの遵守と原告側への支払」を条件に和解)



SFLC、GPL違反で新たに2社を提訴

Software Freedom Law Centerが、オープンソースソフトのライセンス規約違反で、2社を提訴した。

2007年11月22日 09時20分 更新

オープンソースに無料の法的サービスを提供するSoftware Freedom Law Center(SFLC)は11月20日、GNU General Public License(GPL)に違反したとして、通信機器製造販売会社の米Xterasysと米High-Gain Antennasを、米ニューヨーク州南部地区連邦地裁に提訴したことを明らかにした。

争点は、GPL ver
「BusyBox」。GPLv
が、両社はBusyBo
いないという。SFL
支払いと裁判費用

Verizonに「GPL違反」訴訟

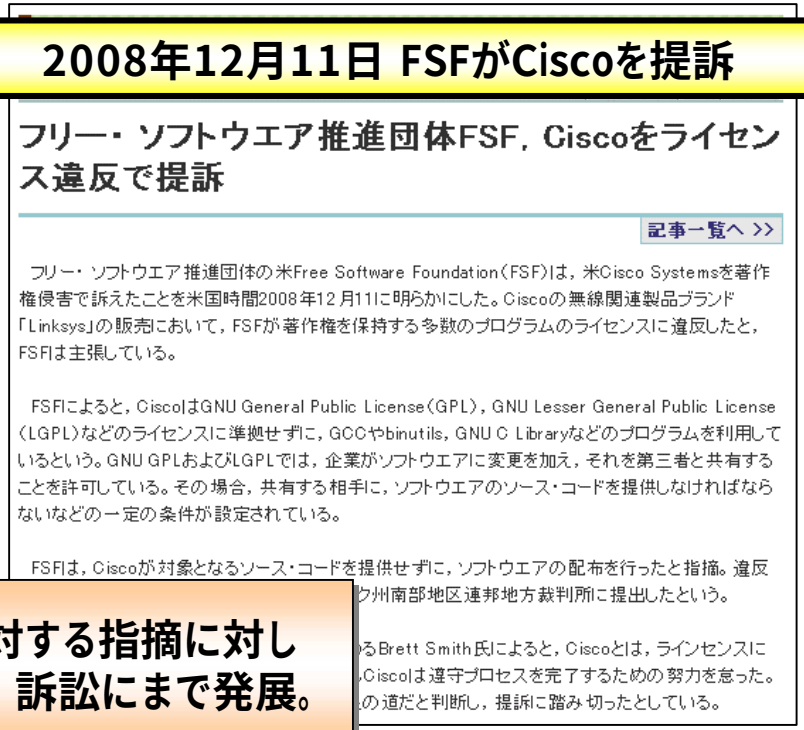
オープンソースソフトのライセンス規約違反で既に3社を提訴したSoftware Freedom Law Centerが、今度はVerizonを相手取る訴訟を起こした。

2007年12月11日 08時49分 更新

オープンソースに無料の法的サービスを提供するSoftware Freedom Law Center(SFLC)は12月7日、オープンソースプログラム「BusyBox」をめぐり、米Verizon CommunicationsをGNU General Public License(GPL)違反で米ニューヨーク州南部地区連邦地裁に提訴したと発表した。同プログラムに関してSFLCが起こした4件目のGPL違反訴訟となる。

Verizonは光ファイバー接続
BusyBoxはGPL version 2 (GPL
公開が義務付けられているが、

2008年12月11日 FSFがCiscoを提訴



フリー・ソフトウエア推進団体FSF，Ciscoをライセンス違反で提訴

記事一覧へ >>

フリー・ソフトウエア推進団体の米Free Software Foundation(FSF)は，米Cisco Systemsを著作権侵害で訴えたことを米国時間2008年12月11日に明らかにした。Ciscoの無線関連製品ブランド「Linksys」の販売において，FSFが著作権を保持する多数のプログラムのライセンスに違反したと，FSFは主張している。

FSFによると，CiscoはGNU General Public License(GPL)，GNU Lesser General Public License(LGPL)などのライセンスに準拠せずに，GCCやbinutils，GNU C Libraryなどのプログラムを利用しているという。GNU GPLおよびLGPLでは，企業がソフトウエアに変更を加え，それを第三者と共有することを許可している。その場合，共有する相手に，ソフトウエアのソース・コードを提供しなければならないなどの一定の条件が設定されている。

FSFは，Ciscoが対象となるソース・コードを提供せずに，ソフトウエアの配布を行ったと指摘。違反
ク州南部地区連邦地方裁判所に提出したという。

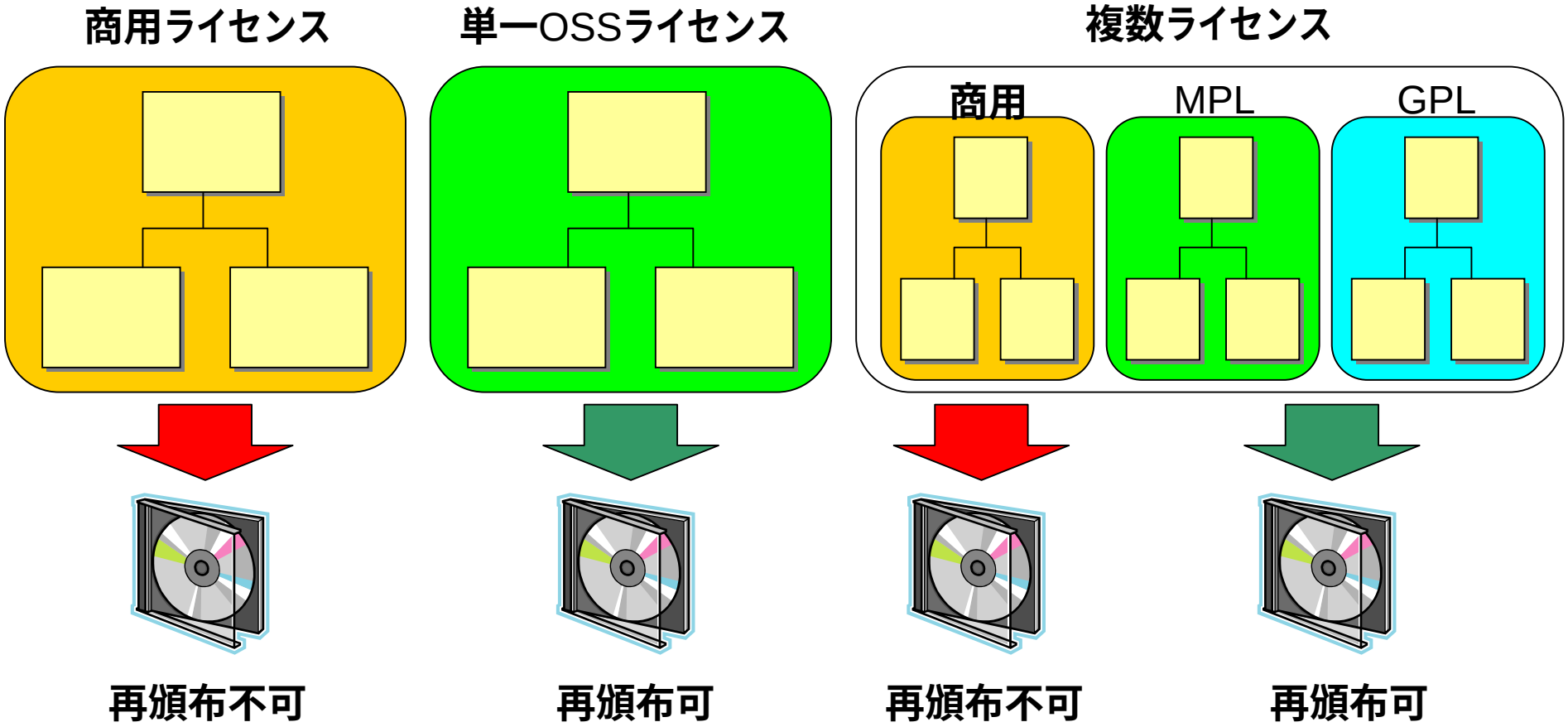
るBrett Smith氏によると，Ciscoとは，ラインセンスに
Ciscoは遵守プロセスを完了するための努力を怠った。
の道だと判断し，提訴に踏み切ったとしている。

いずれも、ＧＰＬ違反の疑いに対する指摘に対し不適切な回答/対応をした結果、訴訟にまで発展。

ライセンス違反を起こさないために①

◆ 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

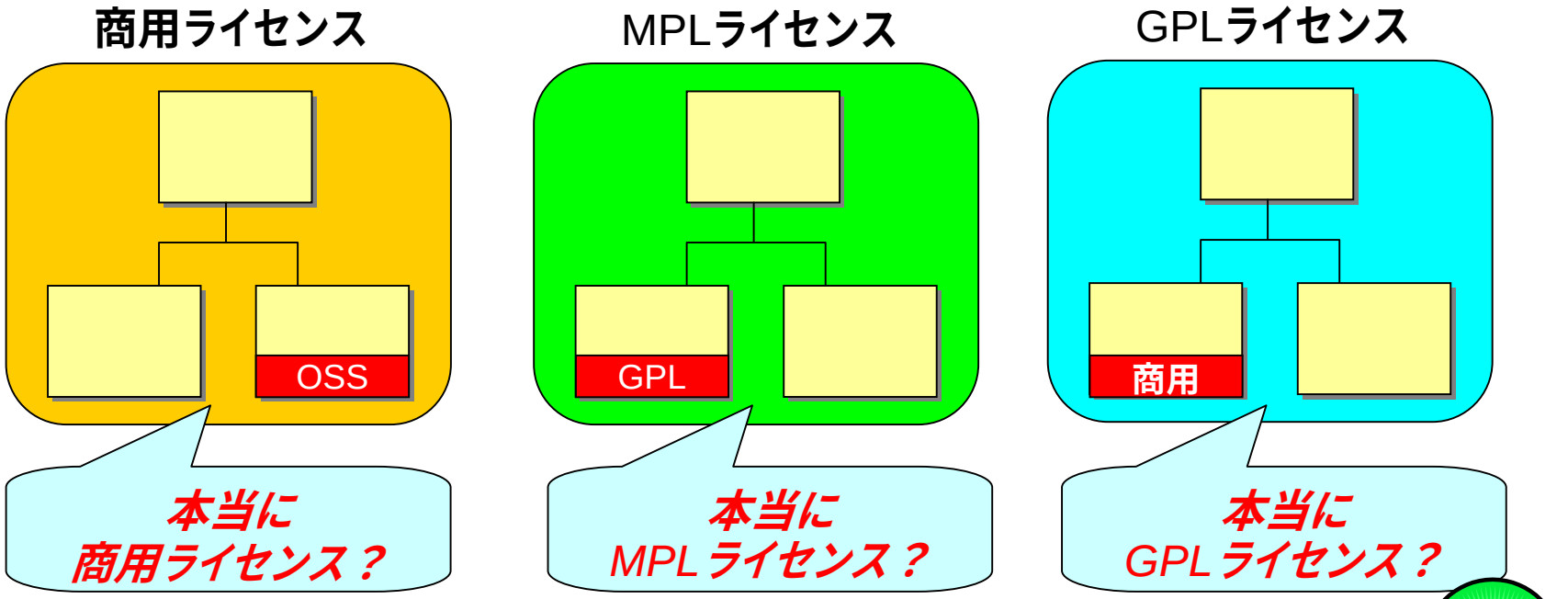
企画･設計段階での OSSポリシー策定



ライセンス違反を起こさないために②

◆ 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



ツール（protexIP）を使った機械的・網羅的なコード検査が必要

参考

protexIPによる検査結果実例

- 対象物件
  - あるベンダの実際の製品
  - 開発規模：約120kL

検出された違反は製品出荷前に是正済み

製品Ver.	検出された違反件数	違反箇所の実装元	違反内容と是正措置

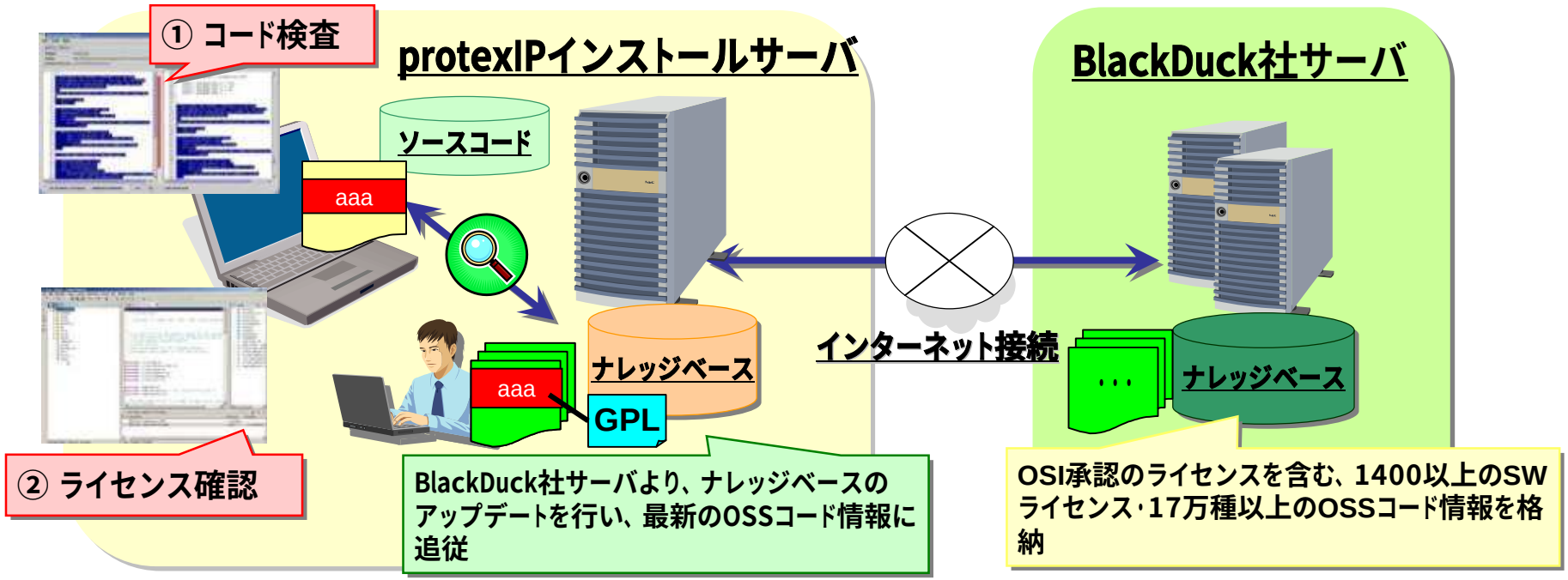
配布資料では非開示とさせていただいております

2．特長･機能ご紹介

機能概要

① **コード検査**
自社物件とOSSコードを比較し、混入または流用の可能性がある箇所を検出。

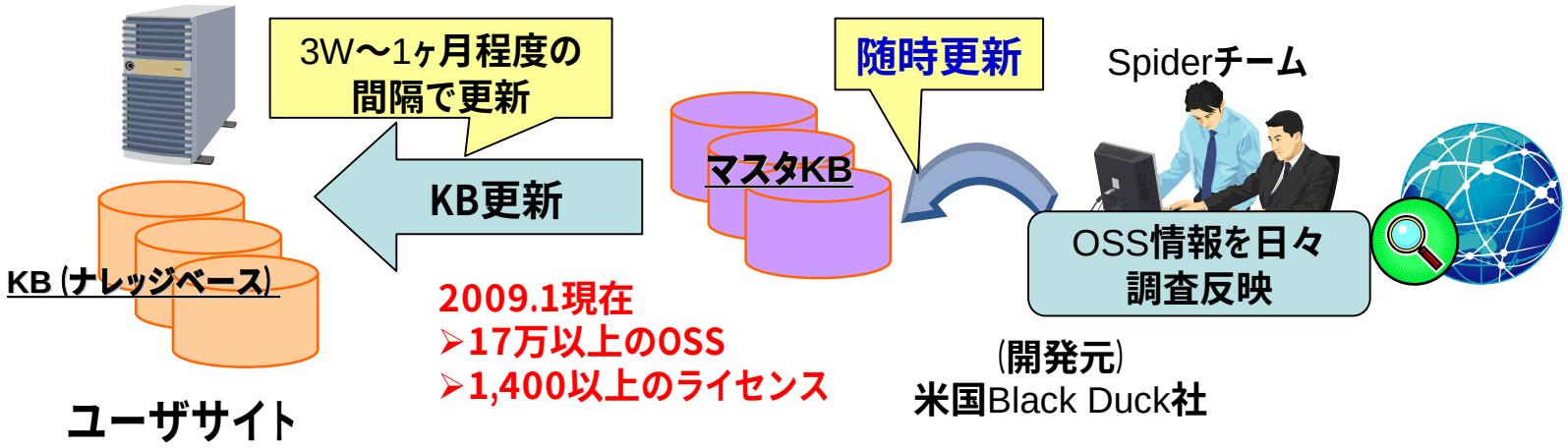
② **ライセンス確認**
検出されたOSSのライセンス条件を確認。



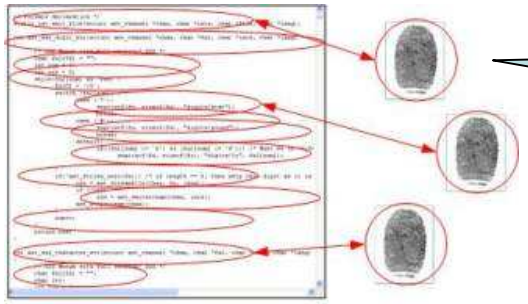
protexIPは、このような検査を実用的な時間・資源で効率的に
実施できるよう様々な工夫がなされています

特長1：高度な検出能力

豊富なOSSとライセンス情報を格納した検証用DB（ナレッジベース）



高速・柔軟な照合が可能なCode Prints



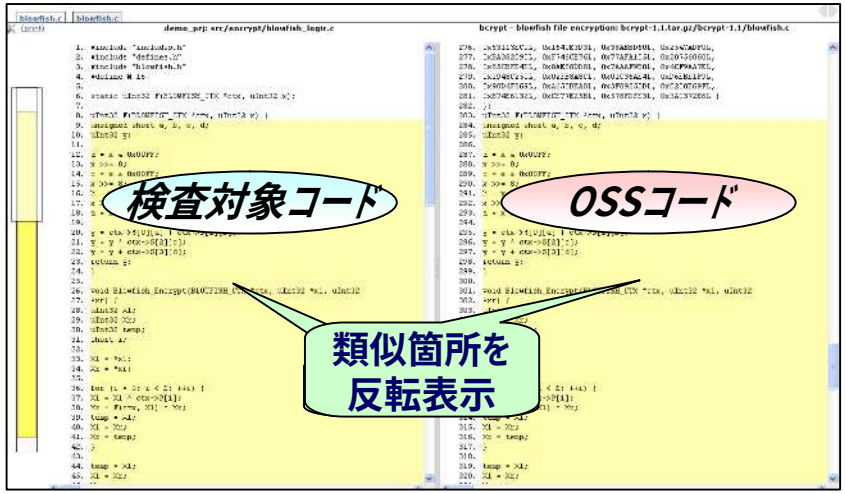
Code Prints：コードの特徴情報を抽出・エンコード

特長

- バイナリファイル（ライブラリ、画像等）にも対応
- データサイズの大幅な縮小、高速な照合
- ファイル単位の流用だけでなく、部分的なコード流用や論理構造の一致も検出

特長2：ライセンス上の問題確認を支援

OSSコード検出箇所の対比確認



類似箇所の実コードを確認し、実際に流用されたのか偶然の一致・一般的実装なのかを判断

互換性の無いライセンスを検出

検査結果画面上の表示

Project: cddl

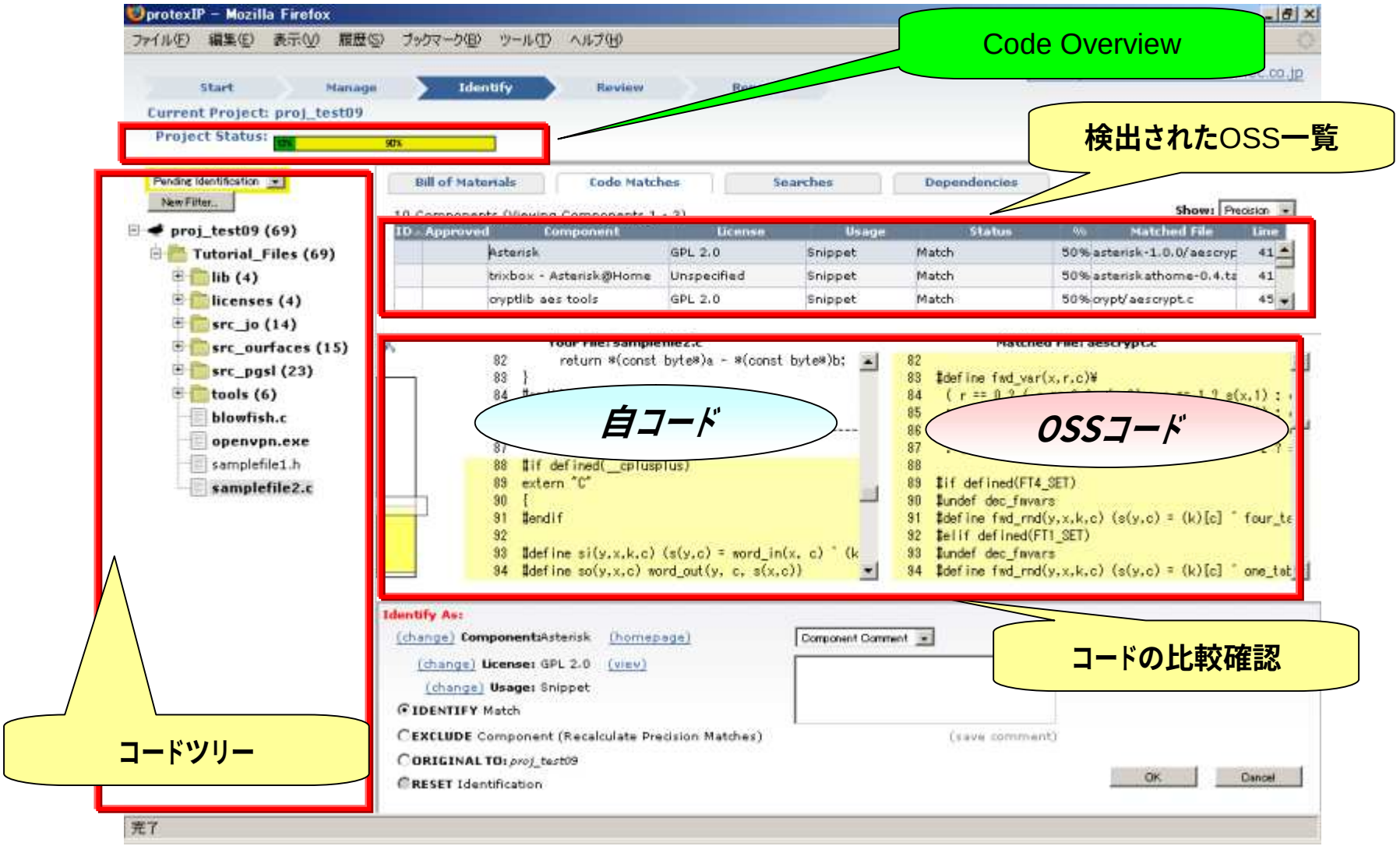
3 Components

Approved	License Conflict	Component	Version	License	Usage	Ship Status	# ID'd	# Depends
N/A	N/A	cddl	Unspecified	COMMON DEVELOPMENT	Original Code	Ship	322	0
✔		Grub	Unspecified	GPL 2.0	Component (S	Ship	247	0
✘	⚠	The GNU Ada compiler	4.0.2	GPL 2.0	Snippet	Ship	1	0

Add a Component...

検出されたOSSのライセンスと互換性が無い（どちらかに違反するため共存できない）ことを警告

画面例



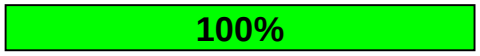
Code Overview

- **プロジェクトの状態を表示 - 検査状況を容易に把握可能**

  - **緑** (No Issues：問題無し)
  - **黄** (Pending Identify：確認待ち)
  - **青** (Pending Approval：承認待ち)
  - **赤** (Violation：問題 = ライセンス非互換あり)

例) 100%自社開発物件 (商用ライセンスで頒布) の場合

① スキャン直後の状態



：OSS検出無し

：OSS検出 ＝ **流用/混入の可能性あり、要確認**

② 検出箇所確認後の状態

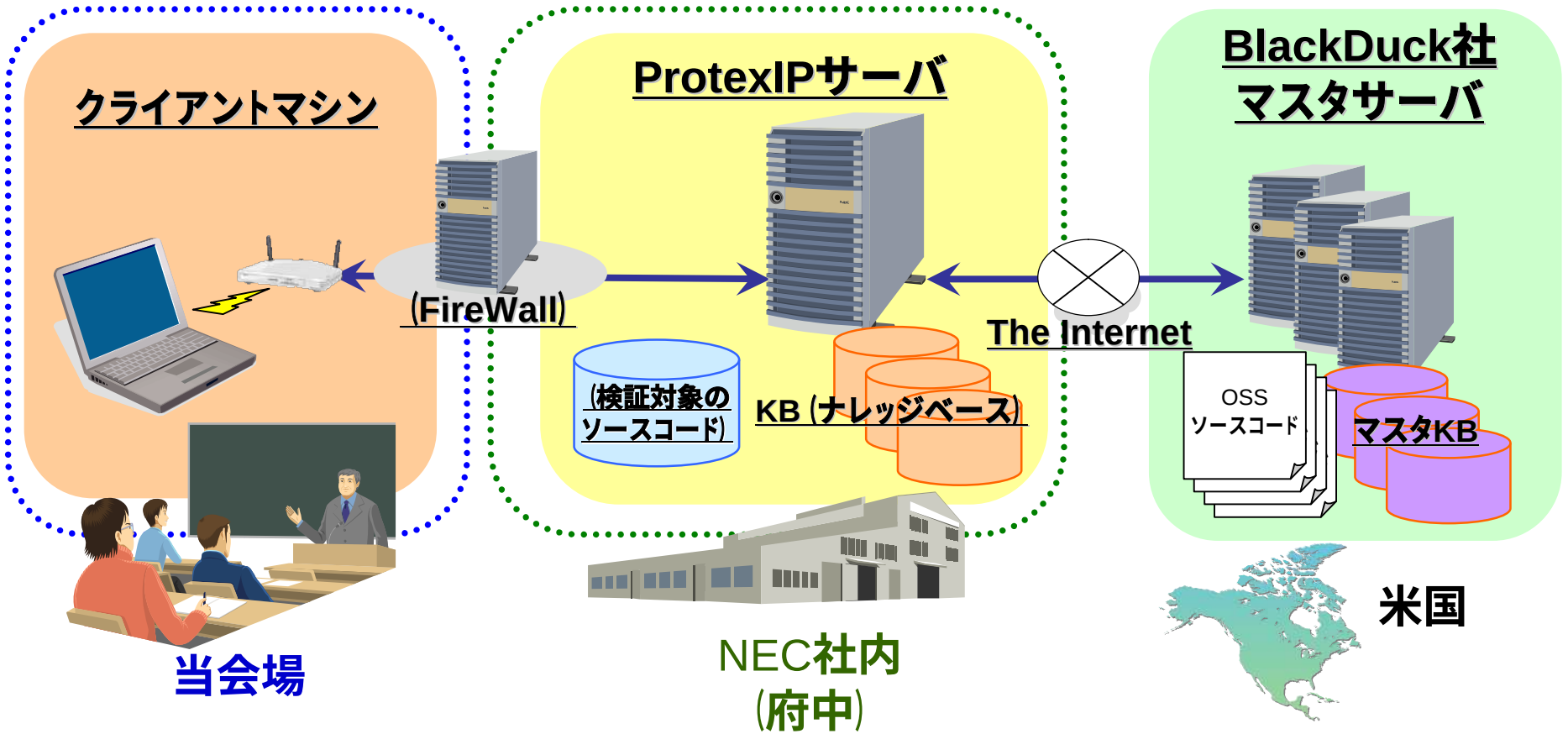
GPL

：ライセンス非互換あり ＝ **このままだとライセンス違反**

BSD

デモンストレーション

デモンストレーション環境



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。

自社導入により蓄積されたノウハウを活用

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

コード検査結果の解説、対処方法判断支援

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

スポット利用のご希望はご相談ください

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

OSSライセンス・コンプライアンス
コンサルティングサービス

社内啓発や、実際の開発物件に対する具体的なご相談に応じます。

サービス内容

OSS活用のリスクについて、部門への啓発から始めたい

「OSS活用におけるリスクと対策」セミナー

開発者/管理者として、具体的な注意事項をチェックしたい

「ソフトウェアライセンスに関わるプログラム開発ガイド」のセミナー

実際の製品について、具体的な相談をしたい

個別相談コンサルティング・サービス

費用等、詳細につきましては以下へお問い合わせください。

E-Mail ： ip-consulting@osspf.jp.nec.com

URL ： http://www.nec.co.jp/oss/IPconsul/

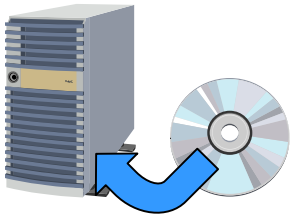
ご試用のご案内

無料

① 評価版ライセンス、② お試しレポート の2種類をご用意。

①評価版ライセンス

- 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

②お試しレポート

- 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

詳細はお手元のご紹介資料をご覧ください。

製品情報・お問い合わせ

- **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 OSSプラットフォーム開発本部 protexIP担当）

Empowered by Innovation

NEC