Empowered by Innovation NEC

OSSコード検出ツール
「Black Duck Protex」を用いた
OSSライセンス違反対策

2012年1月

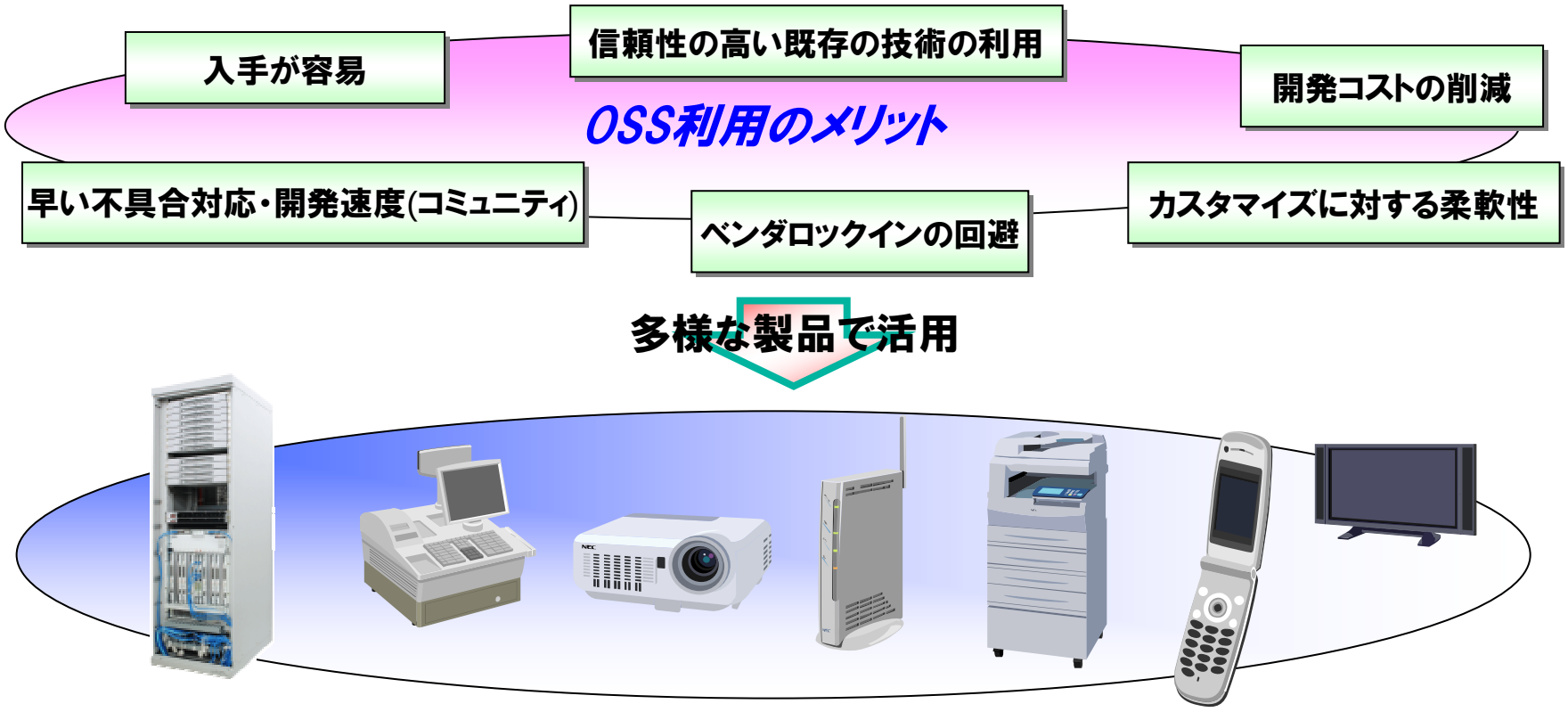
NEC

Contents

Contents

多様な製品で活用されるOSS

- OSS利用には多くのメリットがあり、多様な製品でOSSの活用が拡大。
- 一方でOSSライセンスの理解は充分とはいえず、違反や**訴訟事例**が発生。



OSSとは

OSS(オープンソースソフトウェア)とは

自由に利用できる状態でソースコードが公開されているソフトウェア

- *代表的なOSS:Linuxカーネル、Samba、Apache、PostgreSQL、…*

1. 使用(バイナリを実行すること)は自由。(許諾不要)
2. 利用(複製、改造、再頒布)も自由。
   ただし、著作権者が設定したライセンスに従うことが前提。
   - *代表的なOSSライセンス:GPL、LGPL、MPL、BSD、…*

利用の際の留意事項

- 従うべきライセンス条項をよく確認する。
- 特に二次的著作物のソースコード開示が要求される場合に注意が必要。
  (代表例:GPL)

全体が元のOSSコードの
二次的著作物とみなされる
↓
全体にソースコード開示義務が発生

1. OSSとライセンス

2. **違反事例**

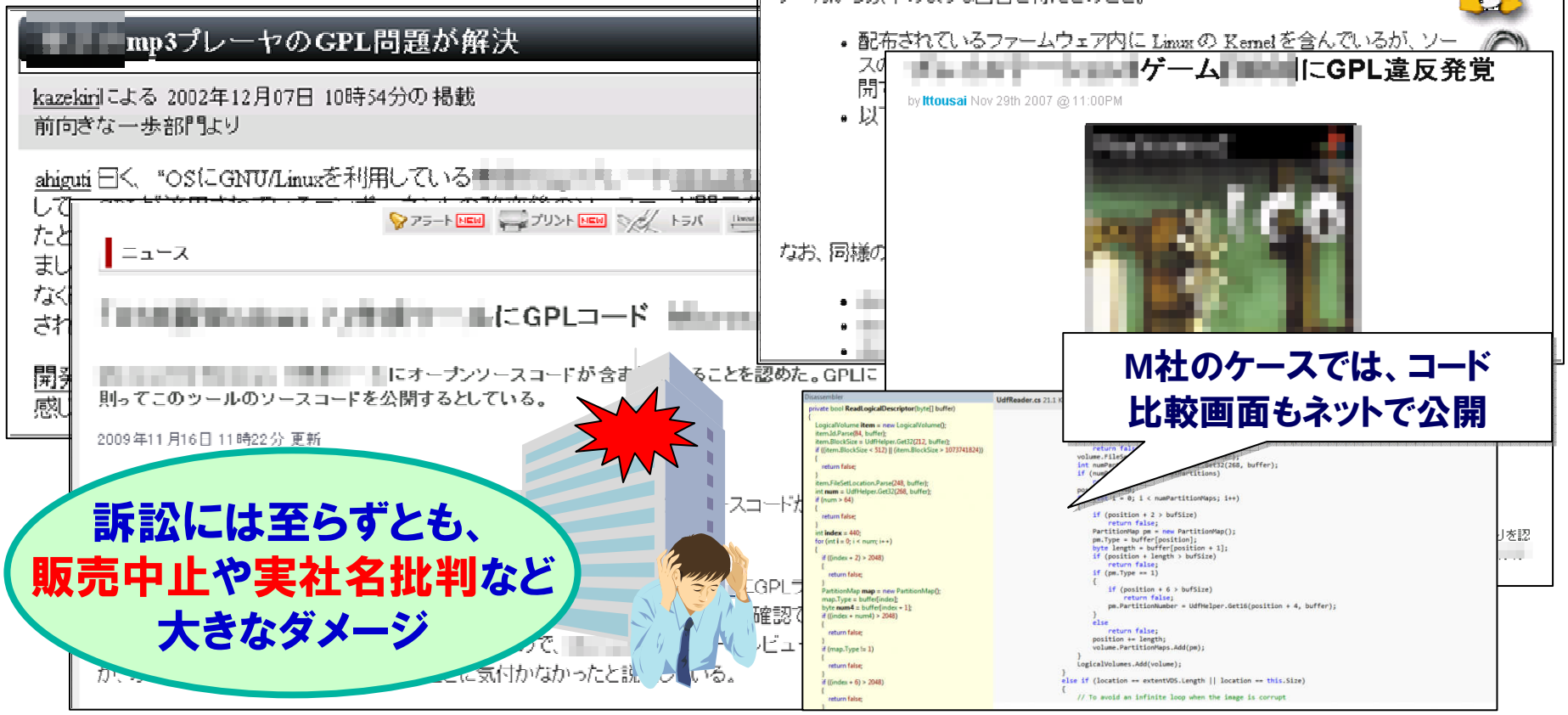
3. **リスク対策のご提案**

4. 「Black Duck Protex」**活用のすゝめ**

違反事例1　～Webサイトで指摘を受けブランドイメージ低下～

- ✓ 2002/11　T社：携帯音楽プレーヤ
- ✓ 2004/4　E社：ルータ
- ✓ 2007/11　S社：ゲームソフト
- ✓ 2009/11　M社：ツール

などなど…

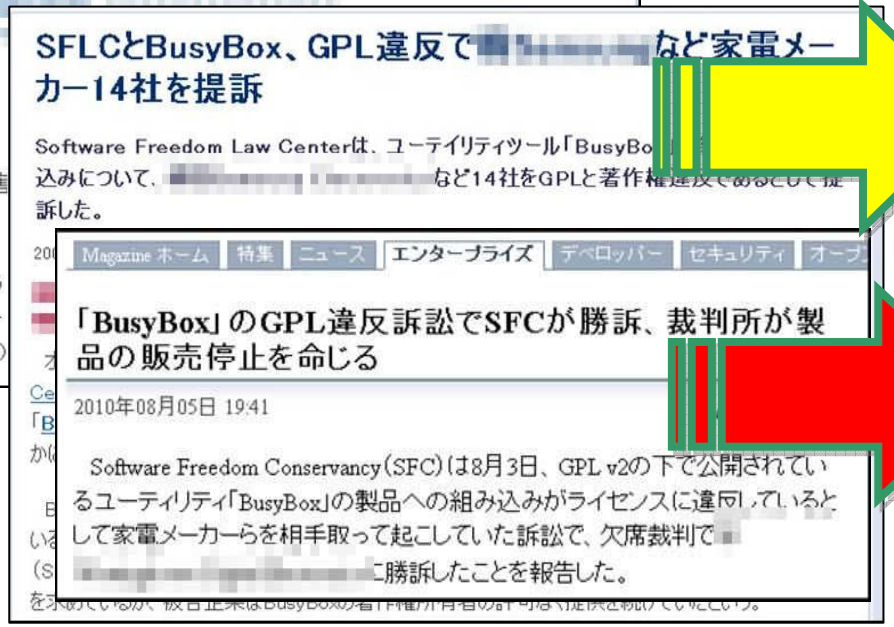


違反事例2　～米国で多数のGPL違反訴訟～

- ✓ 2007/12　V社：無線ルータ
- ✓ 2008/12　C社：無線ルータ
- ✓ 2009/12　S社、V社ほか14社：ルータ、HDテレビ等

などなど…

ほぼ全てがBusyBoxの不正流用によるGPL違反



一部は以下を条件とし和解。
- *GPL遵守（ソースコード開示）*
- *責任者の任命*
- *和解金の支払*

等

2010年8月 欠席裁判でW社が敗訴（一連のGPL違反訴訟で初の判例）
- *販売停止命令*
- *損賠賠償金9万ドル*
- *訴訟費用約4万7千ドル*

1. OSSとライセンス

2. **違反事例**

3. **リスク対策のご提案**

4. 「Black Duck Protex」**活用のすゝめ**

リスク対策のご提案(１)

- ➢ 利用するものは「正しく利用」しましょう。
- ✓ 「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」をご活用ください。

OSSライセンス・コンプライアンス推進フロー

コンプライアンス推進者を設置	OSSライセンス・コンプライアンス(OSSLC)推進者を中心にOSSLC推進会議(コアメンバ)などを設置します。
OSSライセンス教育	リスクの現状を認識し、OSSライセンスを基礎から理解する。一般開発者向け一般教養としての他、次ステップ検討のための共通認識を構築します。
OSS利用ガイドライン作成	自社で主要となるOSSライセンスの理解や対応方針、自社での開発ケースを勘案した注意事項などを記載したガイドラインを作成します。
開発管理プロセス改善	ガイドラインに従ったルールを日常的に遵守するために、開発管理プロセスにチェックポイントを組み込みます。

推進

リスク対策のご提案(２)

- ➢ 利用しているつもりが無くても、「思わぬ流用」は起こりえます。
- ✓ ツールを用いたソースコード検査をお勧めします。

「思わぬ流用」の要因

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

「思わぬ流用」の発見を支援する効果的な手段として、
OSS情報データベースとの比較により、
自社開発物件の中に含まれているOSSを検出するツール
が出てきています。

特に、管理や教育が行き届かない外注・オフショア納品物件への対策としては他に効果的な手段が無い状況。

1. OSSとライセンス

2. 違反事例

3. リスク対策のご提案

4. 「Black Duck Protex」活用のすゝめ

なぜツールが必要か？ なぜProtexか？

開発規模も大きく、人手で確認するのは**事実上不可能**だ。

非常に多くのOSSが存在し、とても**チェックしきれない**。

流用しているOSSは判明したが、**ライセンス違反になるのか**？

Black Duck™ Protex

開発コード内の**OSSコードを検出**

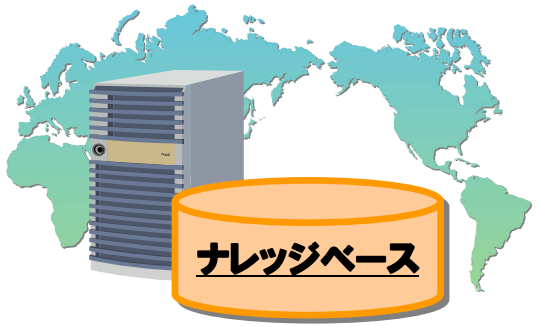
- 高精度な自動スキャン
- 世界最大規模のOSS情報データベースとの照合
- OSSライセンス遵守を支援
- 強力な国内サポート基盤とNEC独自サービス

OSSライセンスのトラブルを未然に防止!!

Protex の特徴

世界最大規模のOSS情報データベースとの照合

著名なOSSサイトとの連携、日々のネット調査により**世界最大規模のOSS情報データベース**を実現。お客様のナレッジベースには**定期的な自動アップデート**で最新情報が反映されます。



独自のマッチング技術による高度な比較技術

独自のマッチング技術により、実用的な時間で**膨大なOSS情報**と**大規模な自社コード**間の一致・類似箇所を検出できます。

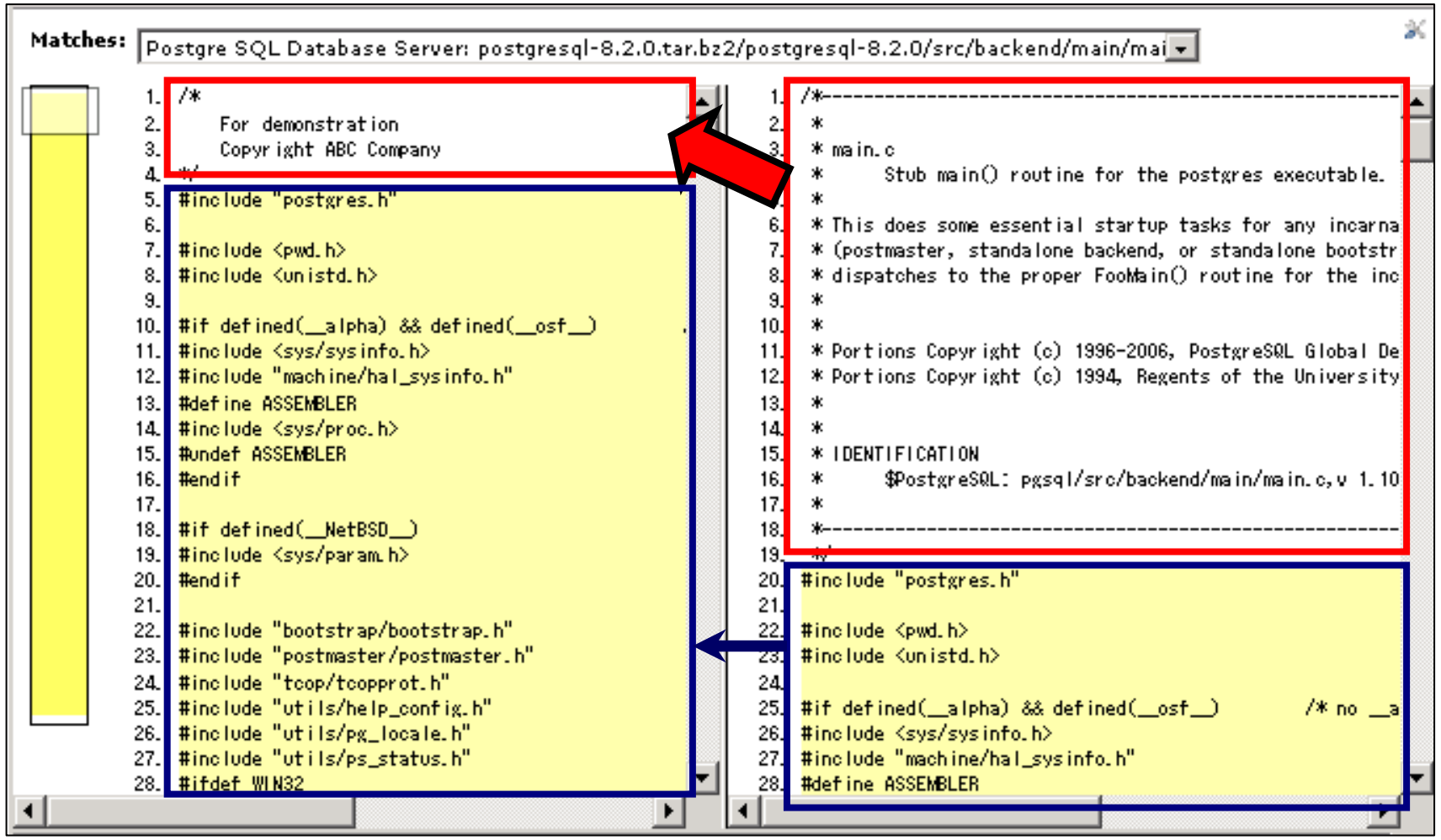
一度のスキャンで、
560,000種類以上の
OSSの全ソースコードとの
総比較確認作業に相当!!

OSSライセンス遵守を支援

共存できないライセンスのOSSが検出されると**「競合」**として表示されるので、**ライセンス違反の判断**に有効です。

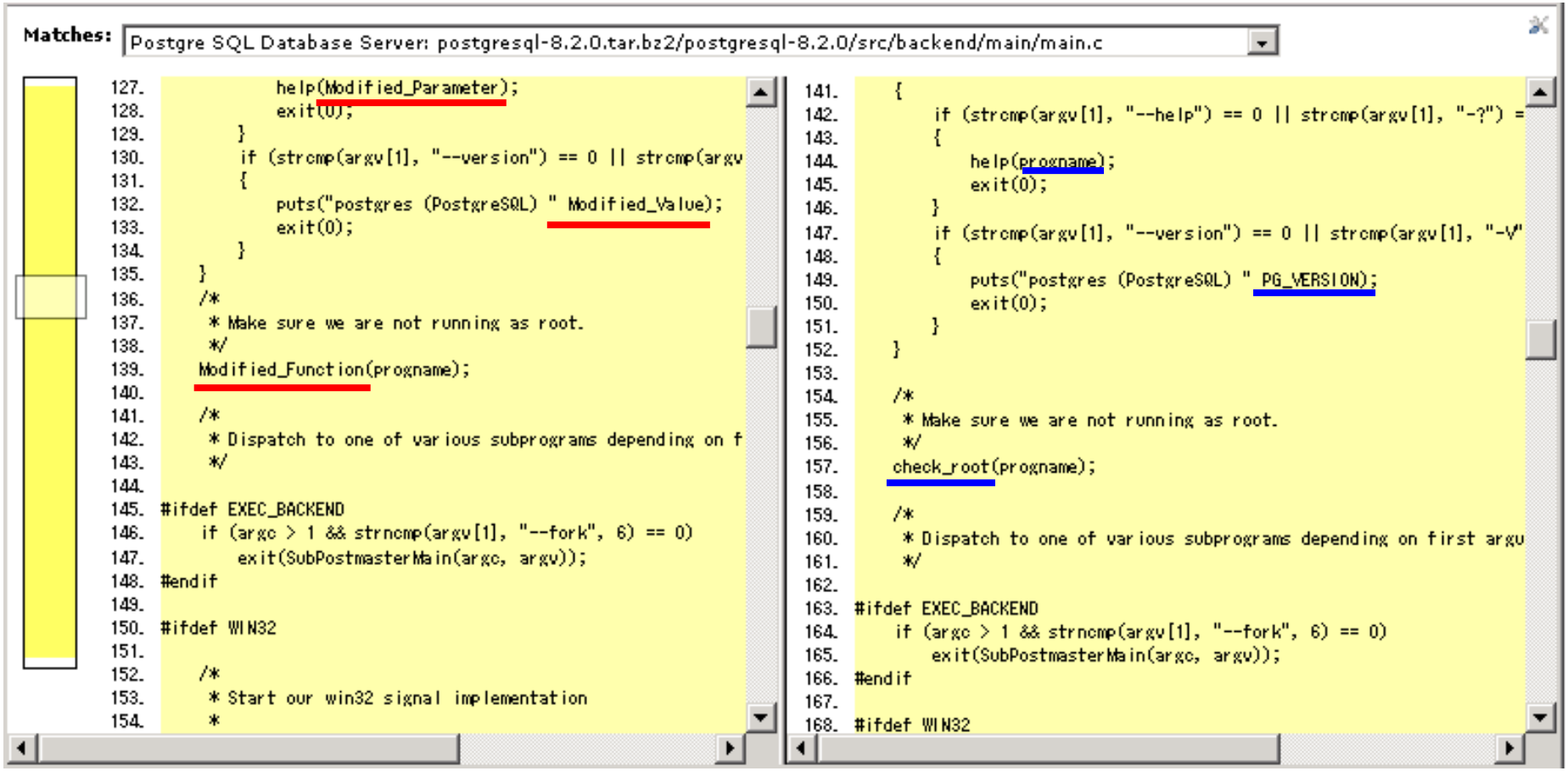
ありがちな流用とProtexによる検出例（１）

◆元ファイル冒頭コメント（copyrightやライセンス名など）を削除し、
自社雛形に置き換え



ありがちな流用とProtexによる検出例（２）

◆元ファイルの関数名や変数名を変更して流用



Protex無料体験のご案内

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。

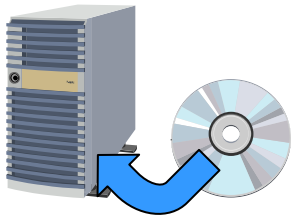
①お試し版レポート

- 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・お問合せは… protexip-info@osspf.jp.nec.com **まで**

Webサイト・お問合せはこちら

- **Black Duck Protex**
  - **Webサイト**
    http://www.nec.co.jp/oss/protexip/
  - **お問合せ**
    E-Mail：protexip-info@osspf.jp.nec.com

- **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**
  - **Webサイト**
    http://www.nec.co.jp/oss/IPconsul/
  - **お問合せ**
    E-Mail：:ip-consulting@osspf.jp.nec.com

Empowered by Innovation