

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

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

Contents

1. OSSとライセンス

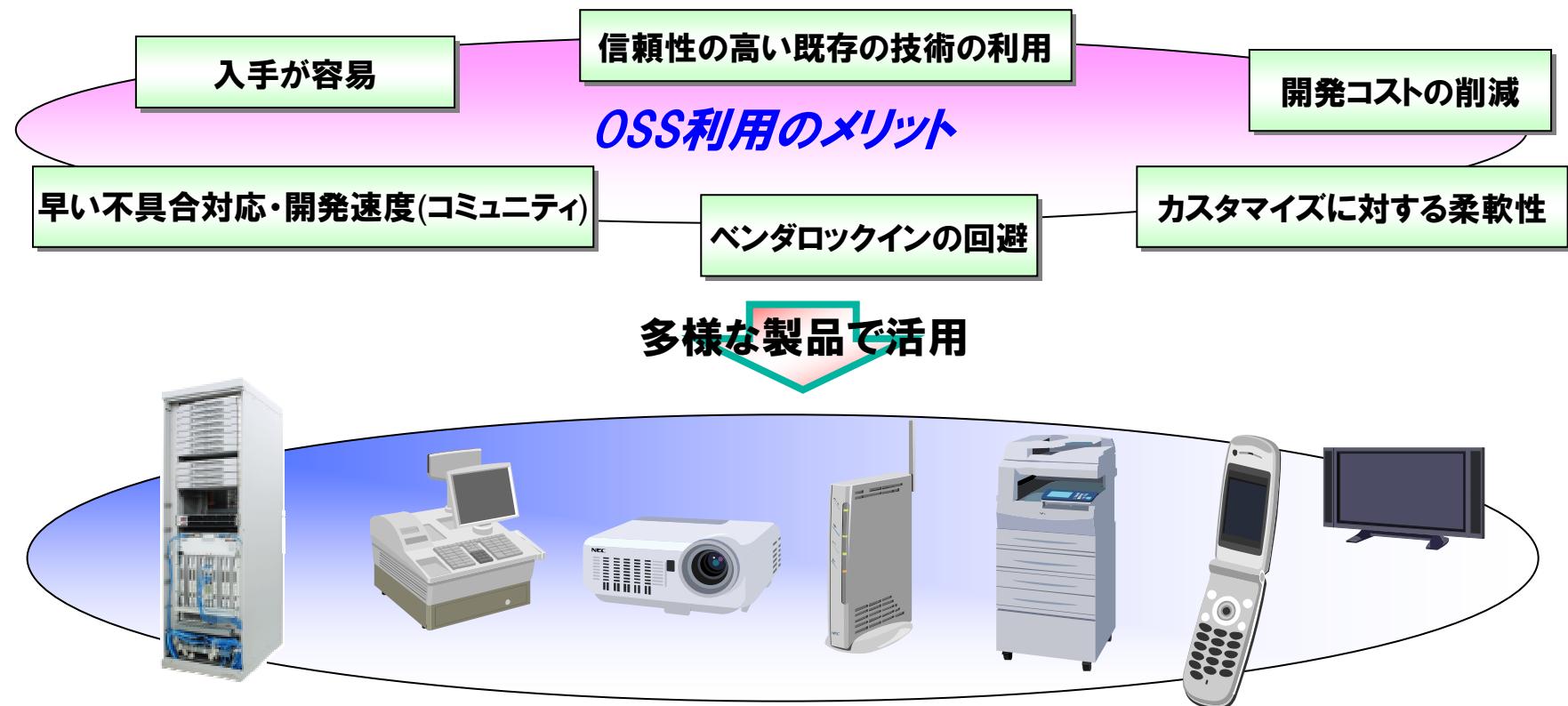
2. 違反事例

3. リスク対策のご提案

4. 「Black Duck Protex」活用のすゝめ

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、…

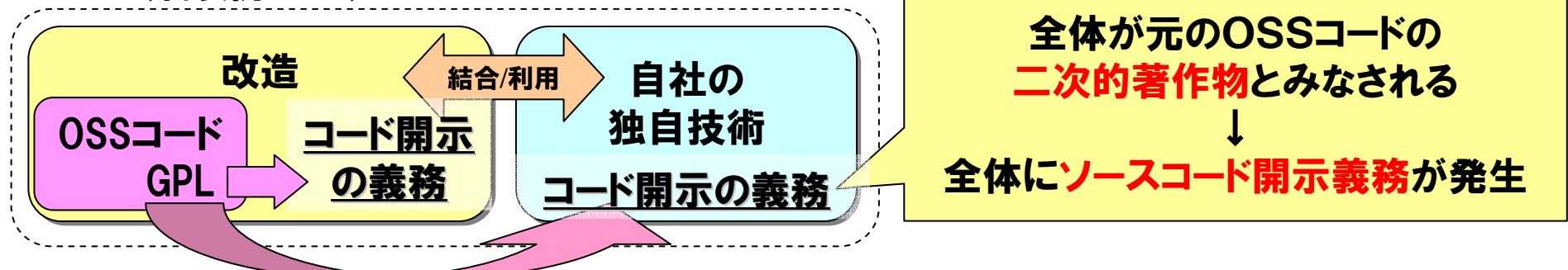
1. 使用(バイナリを実行すること)は自由。(許諾不要)
2. 利用(複製、改造、再頒布)も自由。

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)



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...

mp3プレーヤのGPL問題が解決

kazekirilによる 2002年12月07日 10時54分の掲載
前向きな一步部門より

ahiguti曰く、"OSにGNU/Linuxを利用している...
してたとましましなくされ開発感し" にGPLコード

にオープンソースコードが含まれることを認めた。GPLに則ってこのツールのソースコードを公開するとしている。

2009年11月16日 11時22分 更新

訴訟には至らずとも、販売中止や実社名批判など大きなダメージ



のルータでGPL違反とセキュリティ問題が発覚

wakatonolによる 2004年04月05日 2時31分の掲載
問題てんこもり？部門より

Anonymous Coward曰く、"Tatsuyoshi tech diaryによれば、...
のファームウェアの解析の結果をもってサポートに問い合わせたところ、...
メーカから以下のような回答を得たとのこと。

Anonymous Coward曰く、"Tatsuyoshi tech diaryによれば、...
のファームウェア内にLinuxのKernelを含んでいるが、ソースの開発者曰く、...
ゲーム...にGPL違反発覚

by ittousai Nov 29th 2007 @11:00PM

なお、同様の...
• 配布されているファームウェア内にLinuxのKernelを含んでいるが、ソースの開発者曰く、...
ゲーム...にGPL違反発覚



M社のケースでは、コード比較画面もネットで公開

```
private bool ReadLogicalDescriptor(Byte[] buffer)
{
    LogicalVolume item = new LogicalVolume();
    item.Id.ParseDk(buffer);
    item.BlockSize = UdfHelper.Get32(D12, buffer);
    if (item.BlockSize > 512 || (item.BlockSize > 1073741824))
        return false;
    item.FileGetLocation.ParseD8(buffer);
    int num = UdfHelper.Get32(D98, buffer);
    if (num > 64)
        return false;
    int index = 440;
    for (int i = 0; i < num; i++)
    {
        if ((index + i) > 2048)
            return false;
        PartitionMap map = new PartitionMap();
        map.Type = buffer[index];
        byte num = buffer[index + 1];
        if ((index + num) > 2048)
            return false;
        if (map.Type != 1)
            return false;
        if ((index + 6) > 2048)
            return false;
    }
    if (position + 2 > bufferSize)
        return false;
    PartitionMap newPartitionMap();
    pm.Type = buffer[position];
    byte length = buffer[position + 1];
    if (position + length > bufferSize)
        return false;
    if (pm.Type == 1)
    {
        if (position + 6 > bufferSize)
            return false;
        pm.PartitionNumber = UdfHelper.Get32(position + 4, buffer);
    }
    else
    {
        return false;
        position += length;
        volume.PartitionMaps.Add(pm);
    }
    logicalVolumes.Add(volume);
}
else if ((location == extentVos.Length || location == this.Size))
{
    // To avoid an infinite loop when the image is corrupt
}
```

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

FSF、GPL違反で[...]を提訴

[...]を、無線ルータ製品においてプログラムをライセンスを順守しないで利用しているとして、FSFが提訴した。

2008年12月12日 13時17分 更新 [末岡洋子, SourceForge.JP Magazine]

フリーソフトウェア支援団体のFree Software Foundation (FSF)は米国時間の12月11日、FSFに属する著作権を侵害したとして[...]を提訴したことを明らかにした。FSFは、[...]が無線ルータブランド[...]で、GNU Lesser General Public License (GPL)

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

SFLCとBusyBox、GPL違反で[...]など家電メーカー14社を提訴

Software Freedom Law Centerは、ユーティリティツール「BusyBox」について、[...]など14社をGPLと著作権違反で提訴した。

「BusyBox」のGPL違反訴訟でSFCが勝訴、裁判所が製品の販売停止を命じる

Software Freedom Conservancy(SFC)は8月3日、GPL v2の下で公開されているユーティリティ「BusyBox」の製品への組み込みがライセンスに違反しているとして家電メーカーらを相手取って起こしていた訴訟で、欠席裁判で[...]勝訴したことを報告した。

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
・損害賠償金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。

推進

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。

リスク対策のご提案(2)

- 利用しているつもりが無くとも、「思わぬ流用」は起こります。
- ✓ 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ない状況。

-
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

The screenshot shows a Protex IDE interface comparing two code snippets. The left pane displays the original PostgreSQL source code, and the right pane shows the modified version where the copyright and license comments have been replaced by a company-specific template.

Matches: PostgreSQL Database Server: postgresql-8.2.0.tar.bz2/postgresql-8.2.0/src/backend/main/main.c

Original Code (Left):

```
1. /*  
2.  * For demonstration  
3.  * Copyright ABC Company  
4. */  
5. #include "postgres.h"  
6.  
7. #include <pwd.h>  
8. #include <unistd.h>  
9.  
10. #if defined(__alpha) && defined(__osf__)  
11. #include <sys/sysinfo.h>  
12. #include "machine/hal_sysinfo.h"  
13. #define ASSEMBLER  
14. #include <sys/proc.h>  
15. #undef ASSEMBLER  
16. #endif  
17.  
18. #if defined(__NetBSD__)  
19. #include <sys/param.h>  
20. #endif  
21.  
22. #include "bootstrap/bootstrap.h"  
23. #include "postmaster/postmaster.h"  
24. #include "tcop/tcopprot.h"  
25. #include "utils/help_config.h"  
26. #include "utils/pg_locale.h"  
27. #include "utils/ps_status.h"  
28. #ifdef WIN32
```

Modified Code (Right):

```
1. /*-----  
2. *  
3. * main.c  
4. *      Stub main() routine for the postgres executable.  
*  
5. * This does some essential startup tasks for any incarnation  
* (postmaster, standalone backend, or standalone bootstrap)  
* dispatches to the proper FooMain() routine for the incarnation.  
*  
6. * Portions Copyright (c) 1996-2006, PostgreSQL Global Development Group  
7. * Portions Copyright (c) 1994, Regents of the University of California  
8. *  
9. * IDENTIFICATION  
10. * $PostgreSQL: pgsql/src/backend/main/main.c,v 1.10 2006-02-01 14:00:00  
11. *  
12. *-----  
13. #include "postgres.h"  
14.  
15. #include <pwd.h>  
16. #include <unistd.h>  
17.  
18. #if defined(__alpha) && defined(__osf__)      /* no __alpha  
19. #include <sys/sysinfo.h>  
20. #include "machine/hal_sysinfo.h"  
21. #define ASSEMBLER
```

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

Matches: PostgreSQL Database Server: postgresql-8.2.0.tar.bz2/postgresql-8.2.0/src/backend/main/main.c

```
127.     help(Modified_Parameter);
128.     exit(0);
129. }
130. if (strcmp(argv[1], "--version") == 0 || strcmp(argv[1],
131. {
132.     puts("postgres (PostgreSQL) " Modified_Value);
133.     exit(0);
134. }
135. }
136. /*
137. * Make sure we are not running as root.
138. */
139. Modified_Function(progname);
140.
141. /*
142. * Dispatch to one of various subprograms depending on f
143. */
144.
145. #ifdef EXEC_BACKEND
146.     if (argc > 1 && strncmp(argv[1], "--fork", 6) == 0)
147.         exit(SubPostmasterMain(argc, argv));
148. #endif
149.
150. #ifdef WIN32
151.
152. /*
153. * Start our win32 signal implementation
154. */

141. {
142.     if (strcmp(argv[1], "--help") == 0 || strcmp(argv[1], "-?") =
143.     {
144.         help(proxname);
145.         exit(0);
146.     }
147.     if (strcmp(argv[1], "--version") == 0 || strcmp(argv[1], "-V"
148.     {
149.         puts("postgres (PostgreSQL) " PG_VERSION);
150.         exit(0);
151.     }
152. }
153.
154. /*
155. * Make sure we are not running as root.
156. */
157. check_root();
158.
159. /*
160. * Dispatch to one of various subprograms depending on first argu
161. */
162.
163. #ifdef EXEC_BACKEND
164.     if (argc > 1 && strncmp(argv[1], "--fork", 6) == 0)
165.         exit(SubPostmasterMain(argc, argv));
166. #endif
167.
168. #ifdef WIN32
```

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

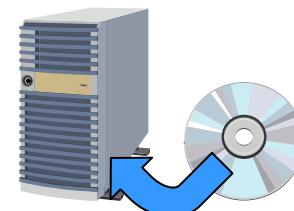
- お客様のソースコード(最大25MB)をお預かりし、スキャン結果をお返します。
- 正規製品の出力との差分はありません。
- 機材のご準備は不要です。



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

NEC