

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

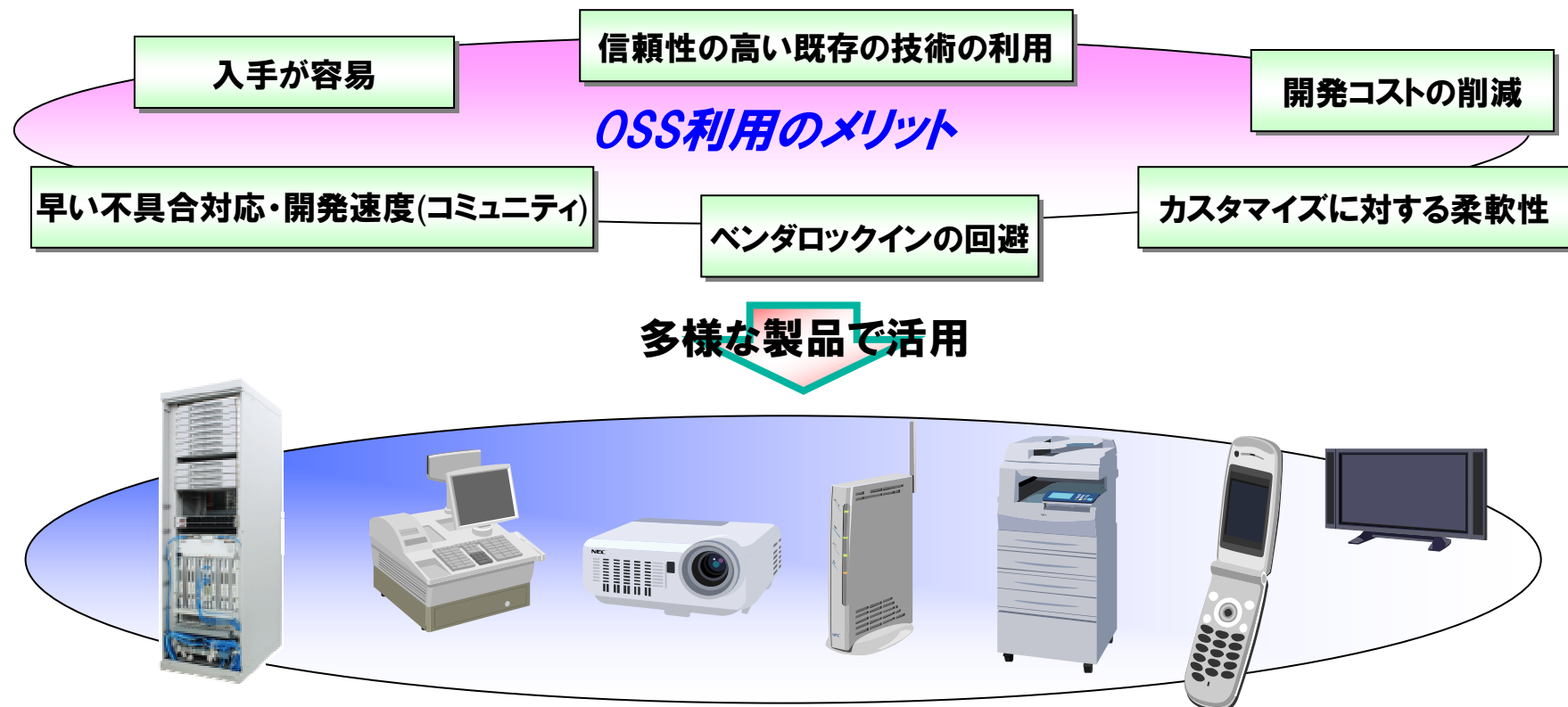
2. 違反事例

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、...

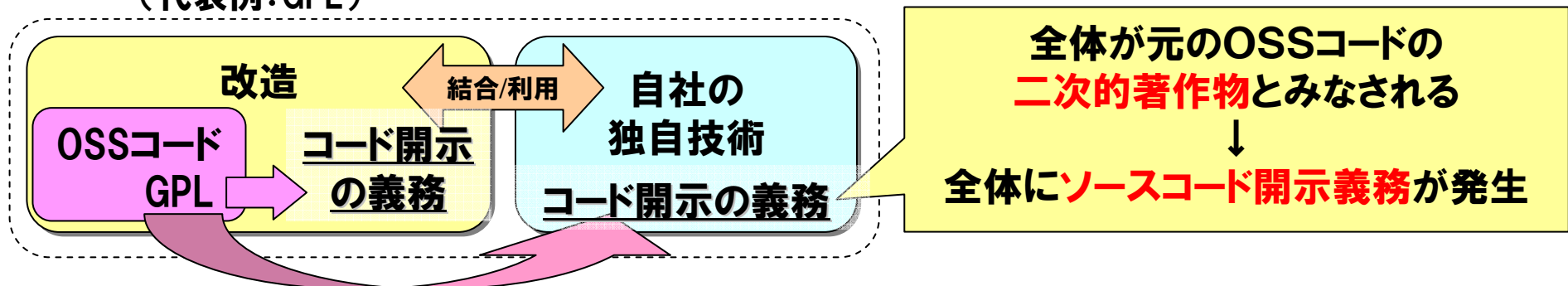
1. 使用(バイナリを実行すること)は自由。(許諾不要)
2. 利用(複製、改造、再頒布)も自由。

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

kazekiriによる 2002年12月07日 10時54分の掲載
前向きな一歩部門より

ahiguti曰く、"OSにGNU/Linuxを利用している"


ニュース

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
問題でんこもり? 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、
メーカーから以下のような回答を得たとのこと。



- 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
- スの
- 開
- 以

by ttousai Nov 29th 2007 @ 11:00PM

ゲームにGPL違反発覚



なお、同様の

•

•

•

**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)
{
    LogicalVolumeItem item = new LogicalVolumeItem();
    item.Parse(buffer);
    item.BlockSize = UdfHelper.Get32(212, buffer);
    if (item.BlockSize < 512 || item.BlockSize > 1073741824)
    {
        return false;
    }
    item.FileSetLocation.Parse(248, buffer);
    int num = UdfHelper.Get32(206, buffer);
    if (num > 64)
    {
        return false;
    }
    int index = 440;
    for (int i = 0; i < num; i++)
    {
        if (index > 2048)
        {
            return false;
        }
        PartitionMap map = new PartitionMap();
        map.Type = buffer[index];
        byte num4 = buffer[index + 1];
        if (index + num4 > 2048)
        {
            return false;
        }
        map.Type = 1;
        if (map.Type != 1)
        {
            return false;
        }
        if (index + 6 > 2048)
        {
            return false;
        }
        LogicalVolumes.Add(volume);
        position += length;
        volume.PartitionMaps.Add(map);
    }
    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[会社名]を提訴

[会社名]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[会社名]を提訴したことを明らかにした。FSFは、[会社名]が無線ルータブランド[会社名]で、GNU Lesser General Public License (GPL)

SFLCとBusyBox、GPL違反で[会社名]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」の組み込みについて、[会社名]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

2010年08月05日 19:41

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主張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[会社名]に勝訴したことを報告した。

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

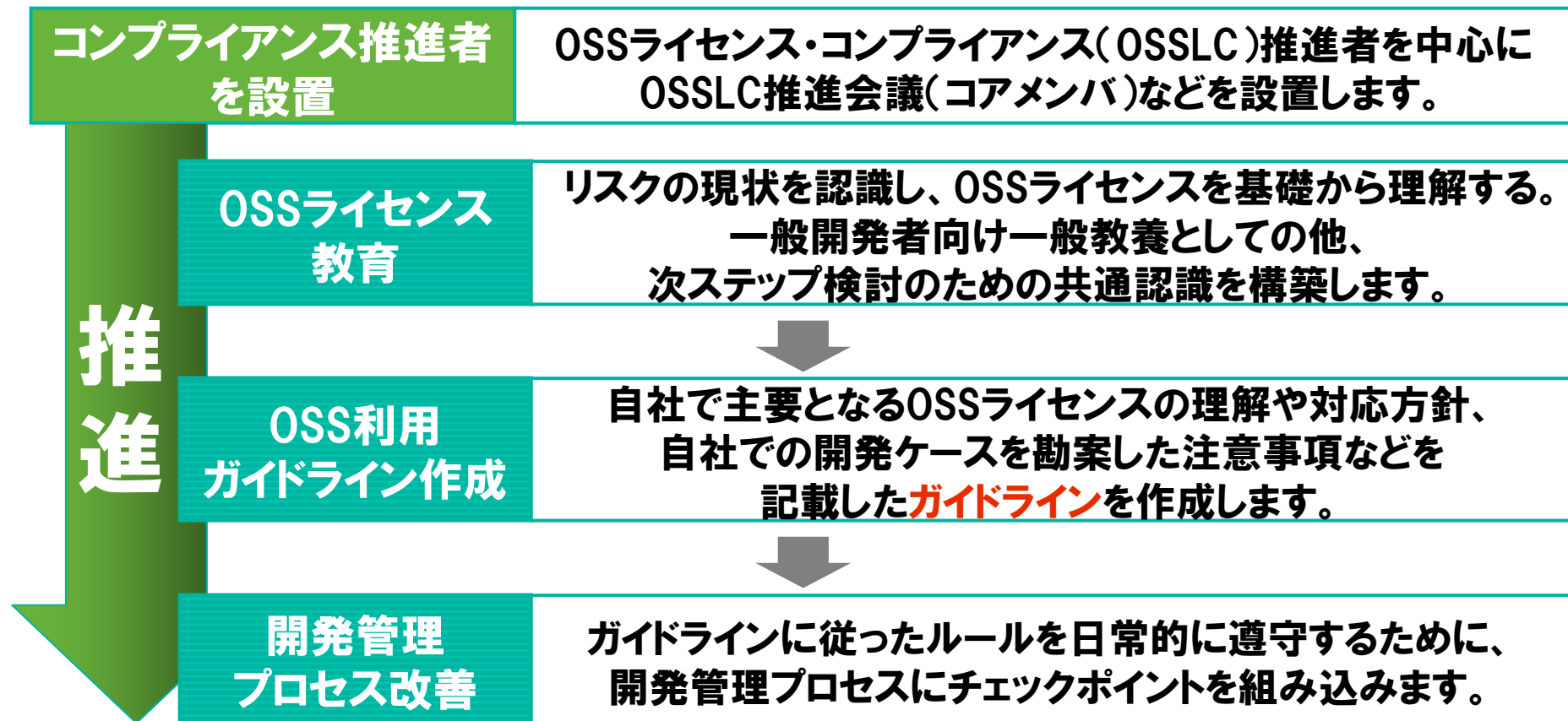
3. リスク対策のご提案

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



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 DuckTM 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

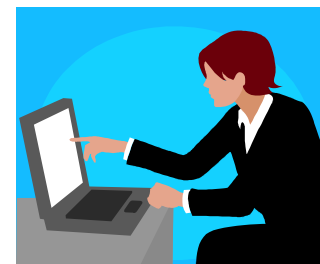
独自のマッチング技術により、実用的な時間で**膨大なOSS情報**と**大規模な自社コード**間の一致・類似箇所を検出できます。

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

Matches: Postgre SQL Database Server: postgresql-8.2.0.tar.bz2/postgresql-8.2.0/src/backend/main/mai

Line	Original Code (Left)	Modified Code (Right)
1	/*	/*-----
2	For demonstration	*
3	Copyright ABC Company	* main.c
4	*/	* Stub main() routine for the postgres executable.
5	#include "postgres.h"	*
6		* This does some essential startup tasks for any incarna
7	#include <pwd.h>	* (postmaster, standalone backend, or standalone bootstr
8	#include <unistd.h>	* dispatches to the proper FooMain() routine for the inc
9		*
10	#if defined(__alpha) && defined(__osf__)	*
11	#include <sys/sysinfo.h>	* Portions Copyright (c) 1996-2006, PostgreSQL Global De
12	#include "machine/hal_sysinfo.h"	* Portions Copyright (c) 1994, Regents of the University
13	#define ASSEMBLER	*
14	#include <sys/proc.h>	*
15	#undef ASSEMBLER	* IDENTIFICATION
16	#endif	* \$PostgreSQL: pgsql/src/backend/main/main.c,v 1.10
17		*
18	#if defined(__NetBSD__)	* -----
19	#include <sys/param.h>	*/
20	#endif	#include "postgres.h"
21		#include <pwd.h>
22	#include "bootstrap/bootstrap.h"	#include <unistd.h>
23	#include "postmaster/postmaster.h"	
24	#include "tcop/tcopprot.h"	
25	#include "utils/help_config.h"	#if defined(__alpha) && defined(__osf__) /* no __a
26	#include "utils/pg_locale.h"	#include <sys/sysinfo.h>
27	#include "utils/ps_status.h"	#include "machine/hal_sysinfo.h"
28	#ifdef WIN32	#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: Postgre SQL 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
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(procname);
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.     * Start our win32 signal implementation
153.     *
154.     */
155.
156.     {
157.         if (strcmp(argv[1], "--help") == 0 || strcmp(argv[1], "-?") =
158.         {
159.             help(procname);
160.             exit(0);
161.         }
162.         if (strcmp(argv[1], "--version") == 0 || strcmp(argv[1], "-v"
163.         {
164.             puts("postgres (PostgreSQL) " PG_VERSION);
165.             exit(0);
166.         }
167.     }
168.
169.     /*
170.     * Make sure we are not running as root.
171.     */
172.     check_root(procname);
173.
174.     /*
175.     * Dispatch to one of various subprograms depending on first argu
176.     */
177.
178.     #ifdef EXEC_BACKEND
179.         if (argc > 1 && strncmp(argv[1], "--fork", 6) == 0)
180.             exit(SubPostmasterMain(argc, argv));
181.     #endif
182.
183.     #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

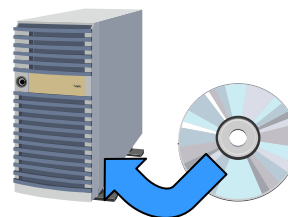
- お客様のソースコード(最大25MB)をお預かりし、スキャン結果をお返しします。
- 正規製品の出力との差分はありません。
- 機材のご準備は不要です。



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@oss pf.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@ossfp.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@ossfp.jp.nec.com

Empowered by Innovation

NEC