.Deb

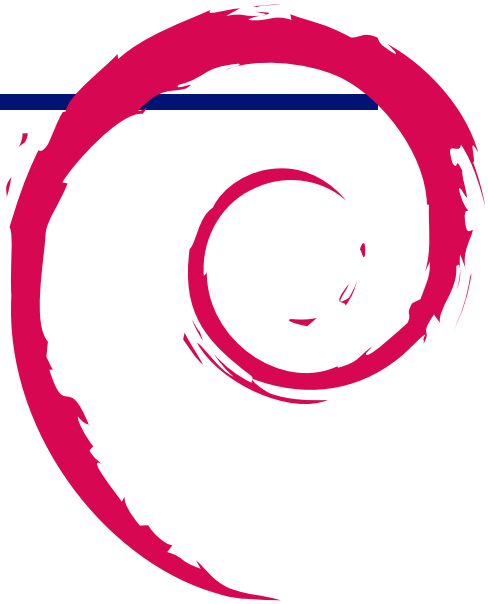
銀河系唯一のDebian専門誌

2015 年 6 月 20 日

特集：Debian と脆弱性対応

デビアン勉強会

目次



1 事前課題

野島 貴英

今回の事前課題は以下です:

1. 本日、何の作業をやるかを宣言ください。
2. (オプション) どこで今回の勉強会の開催を知りましたか？
3. (オプション) 何について聞きたい／参加者と話をしたいですか？

この課題に対して提出いただいた内容は以下です。

1.1 野島

1. Q.hack time に何をしますか？
   A. Nook HD+ をそろそろ debian を動かす件かな？
2. (オプション)Q. 何について聞きたい／参加者と話をしたいですか？
   A. Debian! Debian! Debian!

1.2 pike

1. Q.hack time に何をしますか？
   A. Debian 関連ドキュメント読書
2. (オプション)Q. どこで今回の勉強会の開催を知りましたか？
   A. その他

1.3 wskoka

1. Q.hack time に何をしますか？
   A. mips や tile への移植
2. (オプション)Q. どこで今回の勉強会の開催を知りましたか？
   A. その他

1.4 dictoss

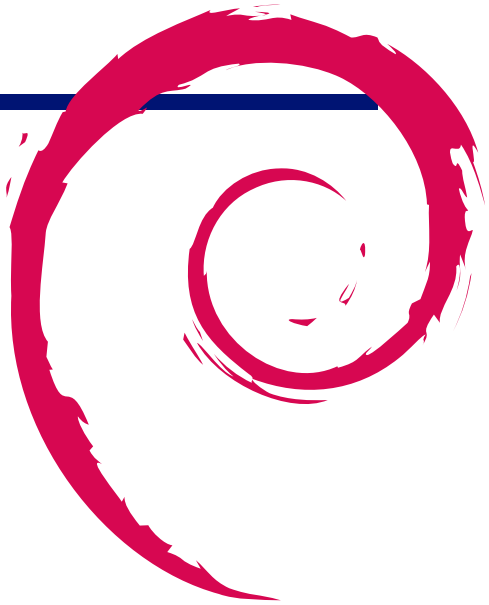
1. Q.hack time に何をしますか？
   A. OSC2015 北海道のブース出展のまとめ、pptp-linux パッケージの kfreebsd 対応
2. (オプション)Q. どこで今回の勉強会の開催を知りましたか？
   A. Debian JP のメーリングリスト

1.5 issei

1. Q.hack time に何をしますか？
   A. 個人で作ってるプログラムの開発を進めたいです。
2. (オプション)Q. どこで今回の勉強会の開催を知りましたか？
   A. その他

1.6 Roger Shimizu

1. Q.hack time に何をしますか？
   A. Debian BTS の勉強
2. (オプション)Q. どこで今回の勉強会の開催を知りましたか？
   A. Twitter (@tokyodebian)



2 Debian Trivia Quiz

野島 貴英

Debian の昨今の話題についての Quiz です。

今回の出題範囲は `debian-devel-announce@lists.debian.org` や `debian-news@lists.debian.org` に投稿された内容などからです。

問題 1. Debian 8.1 がリリースされました。いつだったでしょうか？

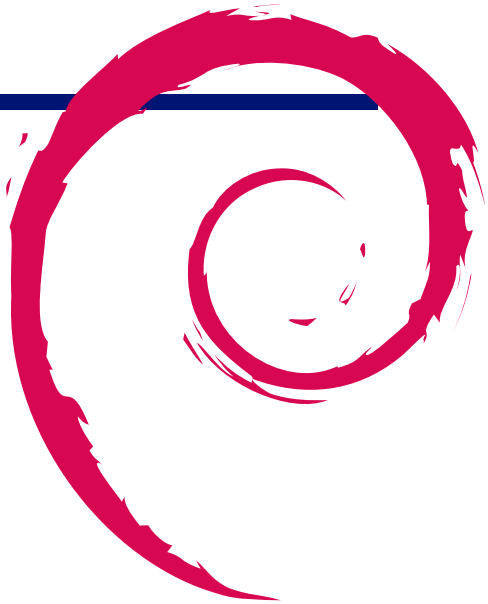
☐ A 2015/6/6
☐ B 2015/6/13
☐ C 2015/6/20

問題 2. 2015/6/10 にて、unstable 版のソースパッケージの数はいくつになったでしょうか？

☐ A 21,000
☐ B 22,000
☐ C 23,000

問題 3. AutomaticDebugPackages の提案とは何？

☐ A 大統一 Debian の岩松さんのデバッグパッケージの件を実施する
☐ B 自動でデバッグ出来るようにする
☐ C -dbg パッケージを止め、.ddeb パッケージを作る



3 最近の Debian 関連のミーティング報告

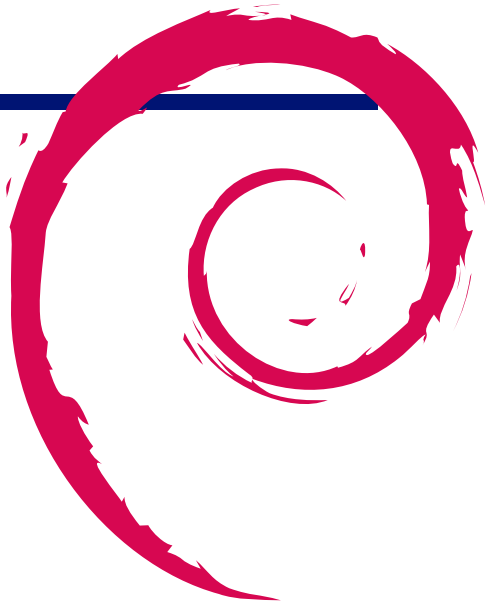
野島 貴英

3.1 第 126 回東京エリア Debian 勉強会

- 場所はスクウェア・エニックスさんのセミナルームをお借りしての開催でした。
- 参加者は 6 名でした。
- セミナ内容は野首さんによる「自然言語処理チーム (pkg-nlp-ja) とパッケージ」でした。
- 残りの時間で hack time を行い、成果発表をしました。
- 宴会の代わりに、「まいどおおきに食堂」で夕食会をやりました。

セミナは野首さん（Debian 公式開発者）による、自然言語処理プログラムの動作に纏わるいろいろなお話を聞かせていただきました。自然言語処理の基礎になっている、辞書のデータ構造、アルゴリズムについての紹介が主な内容でした。普段、自然言語処理の詳細に触れることが無い人にとっては、非常に新鮮な内容だったと思います。

何気ない日本語の処理を Debian で行う場合でも、こういったプログラムの力を借りる事も多いと思います。自然言語処理のパッケージの処理、重要さについて、より広く知られるようになると良いと思いました。



4 Debian と脆弱性対応のあれこれをまとめてみた

野島 貴英

4.1 はじめに

コンピュータセキュリティの勉強会にて登壇を頼まれました。ちょうど良かったので、Debian の脆弱性対応をおさらいして、発表してみることにします。

4.2 Debian のセキュリティチーム

Debian パッケージの脆弱性問題を専門に扱っている心臓部のチームの連絡先は以下の通りです。

- security@debian.org または
- team@security.debian.org

4.3 脆弱性に関する ML

Debian の脆弱性に関するアナウンス・議論が行われている ML は次のとおりです。

- Debian パッケージのセキュリティに関するアナウンス
  debian-security-announce@lists.debian.org
  アーカイブ：
  `https://lists.debian.org/debian-security-announce/`
- Debian パッケージの脆弱性に関するオープンな議論
  debian-security@lists.debian.org
  アーカイブ：`https://lists.debian.org/debian-security/`

4.4 脆弱性対応が行われないアーカイブエリア

Debian パッケージ群は、main/contrib/non-free のアーカイブエリアでそれぞれ提供されています。実は、脆弱性対応について、contrib/non-free のアーカイブエリアのパッケージについては、基本的に除外されています。

こちらの理由としては、contrib と non-free に収められたソフトウェアのライセンスの問題によります。これらのソフトウェアはライセンスの都合上、勝手に直すことが許諾されていない場合があるためとなります。もちろん、contrib と non-free であっても、ライセンス上、直しても良いものもあり、こちらについては通常の通りセキュリティチームにて脆弱性対応が図られることがあります。

4.5 脆弱性に関しての対応の流れ

Debian ユーザあるいは Debian の関係者にかかわらず、もし脆弱性の問題を見つけたら、

PAT1: 既知の問題 (公開済脆弱性情報) の場合は、security タグをつけて BTS してください。
PAT2: 既知でない場合は、そっと security@debian.org または team@security.debian.org にメールで連絡 (英文) し、あとは指示に従えば良いです。

もちろん、脆弱性対策パッチも書いたのであれば、報告の際にパッチも一緒に送ると喜ばれます。

4.5.1 既知の脆弱性でない場合の動き

既知の脆弱性でない場合、セキュリティチームは Debian 以外のベンダ（ディストリビューション等含む）関係者らにも脆弱性情報が共有され、CVE などの脆弱性情報データベース登録にも協力する動きが取られます。

4.5.2 既知の脆弱性の収集

Mitre 社 (CVE の DB を管理している会社）から、CVE の情報を定期的に取り込んでいます。こちらの情報に基づき、Debian に関係ある・なし、重要度を判定して仕分けされ、バグ追跡システムに登録していく仕組み（インフラ）があります。

4.6 脆弱性対応状況の確認方法

以下のサイトで状況を確認できます。

1. セキュリティ観点から確認したい場合
   - `https://security-tracker.debian.org/tracker/`
   - 様々な視点から、巷の脆弱性データベースと Debian の各パッケージの対応状況を確認可能です。
2. QA 観点から確認したい場合
   - `https://tracker.debian.org/`
   - Debian パッケージについて、現在のバグの修正状況、パッケージのリリース状況がパッケージ毎にわかります。
3. BTS した・されたものを確認したい場合
   - `https://bugs.debian.org/`
   - BTS した結果がどう扱われているか、進行しているか確認できます。

4.7 その他トピック

以上で、まとめとしては終わったので、昨今の Debian のセキュリティに関するトピックをいくつか紹介します。

4.7.1 hardening

C/C++ で書かれたプログラムについて、gcc の機能を活用して、セキュリティ強化を行った Debian パッケージを作る試みです。hardening 有効時、ビルド時に実際に付け加えられる gcc のオプションは以下の通りです。

```
-fstack-protector-strong -Wformat -Werror=format-security -D_FORTIFY_SOURCE=2
```

4.7.2 Debian パッケージ済みの脆弱性静的解析ツール群

Debian でパッケージ済の脆弱性静的解析ツール群があります。

項番	パッケージ名	概要
1	flawfinder	C/C++ にてセキュリティ上問題の起きそうな部分を指摘。
2	rats	C, Perl, PHP, Python のコード上問題の起きそうな部分を指摘。
3	pscan	C/C++ にて format 文の文字列について問題の起きそうな部分を指摘。

表 1　Debian パッケージ済み脆弱性静的解析ツール

4.7.3　lintian

lintian は、Debian パッケージについて、自動でスキャンして問題点を解析して警告してくれるツールであり、ある程度のセキュリティ対策の為の対応がパッケージ開発にあたり必須になっており、こちらが過不足なく行われているかをスキャンして開発者に教えてくれます。

昨今にて搭載されたセキュリテイ対応の例として、梱包されているドキュメントに HTML ソースがあった場合、外部リンクが含まれているかをスキャンする事が追加されました。これは、もし、パッケージに含まれるドキュメントが HTML であった場合に、外部リンクへアクセスするようなタグが混ざっているような事が無いようにします。もし、そういったタグやリンクが残っていると、ドキュメントをブラウザで開いた時に、うっかり悪意のあるサイトへ自動的に誘導されてしまうのを防ぎます。

4.7.4　systemd

systemd にはセキュリティに関して強化を図ることが出来るオプションがいくつもあります。こちらをどう活かして、systemd の*.service ファイルを作るかというお話です。

良い文章として、「Security Features in systemd」`http://0pointer.net/public/systemd-nluug-2014.pdf` がありますので、見てみるとよいでしょう。

4.7.5　Reproducible Builds

Debian の 22,000 を超えるソースパッケージを一旦再ビルドし、すでに配布されている Debian パッケージのバイナリと照合する試みの事です。こちらにより、Debian パッケージにいつの間にか悪意のあるバイナリが含まれているような事が無いかをチェックするのが狙いです。Debian の他にも、Fedora/OpenSUSE/NixOS でも行われているとのことです。

詳しくは、

Debian　`http://reproducible.alioth.debian.org/presentations/2014-02-01-FOSDEM14.pdf`
Fedora　`http://securityblog.redhat.com/2013/09/18/reproducible-builds-for-fedora/`

を参照ください。

4.7.6　LTS(Long Time Support)

Debian の各バージョンについて、セキュリティアップデートについてのサポート切れまでの期間を 3 年→ 5 年へ延長する試みです。但し、数万もあるソフトウェア全部について 5 年もサポートするのは非現実的なので、限られたパッケージのセキュリティアップデートのみ延長します。

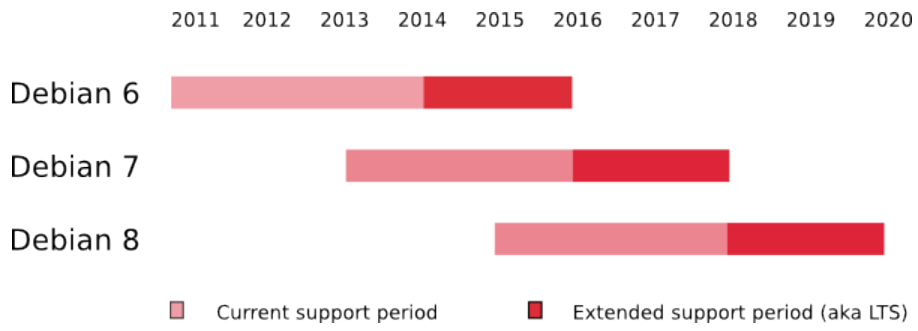


図 1　LTS のサポート期間

LTS は無料でも利用できる一方、有償サポート契約も用意されています。Freexian 社と有償サポート契約を行うのですが、払った値段に応じて、サポートしてくれるパッケージの選択の要望が通りやすくなるという特典があるようです。日本の会社にて契約締結実績は GREE 社があります。

有償サポート契約について詳しくは「Debian Long Term Support」`https://www.freexian.com/en/services/debian-lts.html` を参照ください。

4.7.7　debian-security-support パッケージ

debian-security-support パッケージを導入し、check-support-status コマンドを実行すると、現在お使いの Debian 機に導入されいているパッケージの脆弱性のサポートについて、サポート切れ、もしくは、何らかの理由により脆弱性対策にあたり制限を加えざるを得なかったもののリストが取れるようになりました。

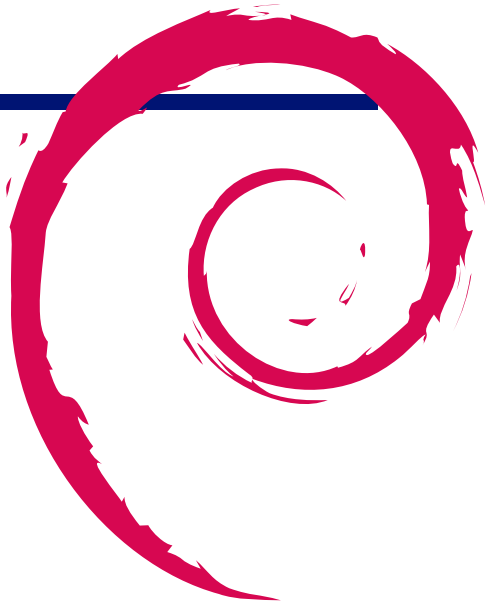
このコマンドの動作としては、

- /usr/share/debian-security-support/security-support-ended
- /usr/share/debian-security-support/security-support-limited

に記載されたパッケージのサポート状況に関する制限の情報と、実際に導入されていてるパッケージ名を照合することにより動作します。もし、これらのファイルから、制限があるパッケージがマシンに見つかった場合は、警告を出してくれます。なお、LTS では、どこまでパッケージについて、脆弱性対応のサポートがなされているかの確認ができます。

4.8　おわりに

Debian の脆弱性対応についてまとめてみました。Debian のセキュリティ維持の為、様々な努力が払われていることがわかりました。



5　会場での無線 LAN のつなぎ方

野島 貴英,Roger

5.1　はじめに

今回試験として、会場側でフィルタ無しのグローバル回線を用意しました。ただ、会場側のセキュリティポリシーにより、wpa-psk AES hidden SSID という方式での提供となります。

以下に Debian マシンでの接続方法を記載します。

また、自分の環境では違うやり方でつながったという方は、野島まで教えて下さい。こちらでもノウハウとして溜めていく予定です。

5.2　wpasupplicant 及び/etc/network/interfaces を利用の場合

もっとも良いマニュアルは、/usr/share/doc/wpasupplicant/README.Debian.gz となります。困った場合はこちらも合わせてご参照下さい。

以下に/etc/network/interfaces の定義について会場の例を記載します。

```
$ sudo vi /etc/network/interfaces
-----以下のエントリがなければ追記ここから----------
iface wlan0_debian inet dhcp
     wpa-conf /etc/wpa_supplicant/wpa_supplicant_debian.conf
-----以下のエントリがなければ追記ここまで----------
$ sudo vi /etc/wpa_supplicant/wpa_supplicant_debian.conf
-----以下のエントリを追記ここから----------
network={
     ssid=<<会場の SSID>>
     psk=<<会場のパスワード>>
     scan_ssid=1
}
-----以下のエントリを追記ここまで----------
$ sudo chmod 600 /etc/wpa_supplicant/wpa_supplicant_debian.conf
$ sudo ifup wlan0=wlan0_debian
```

また、ハマってしまった時のデバッグ方法は、/usr/share/doc/wpasupplicant/README.Debian.gz 中の”4. Trubleshooting” の章が便利です。

5.3　その他の無線 LAN 用パッケージを利用の場合

すみません、自分が情報を持たないため、現場で教えて下さい。

Debian 勉強会資料

2015 年 6 月 20 日　　初版第 1 刷発行

東京エリア Debian 勉強会 （編集・印刷・発行）