

A large, stylized pink brushstroke graphic that forms a partial circle, framing the central text.

東京エリア Debian 勉強会


第 127 回 2015 年 6 月度

野島貴英

2015 年 6 月 20 日

設営準備にご協力ください。

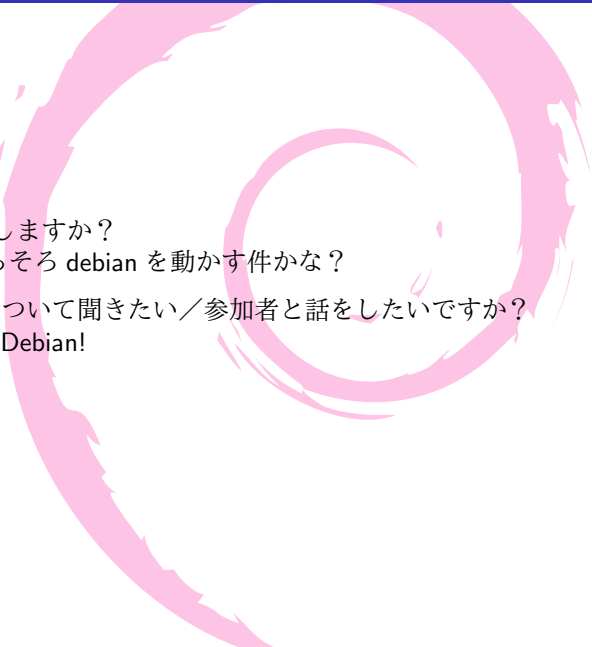
会場設営よろしくおねがいします。

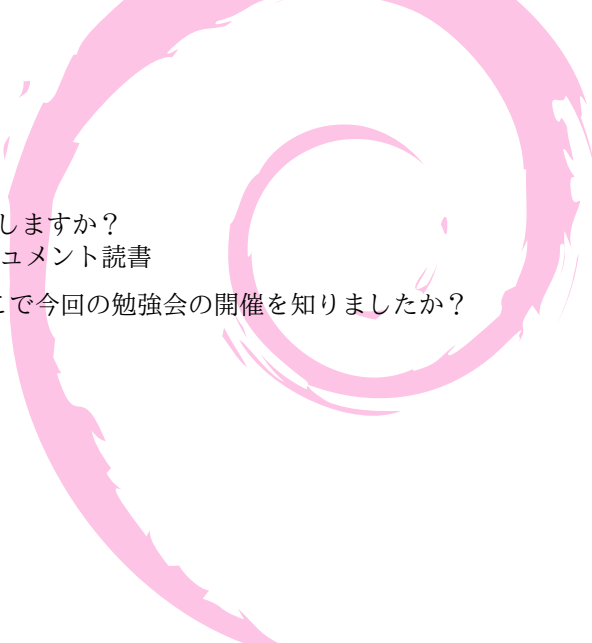


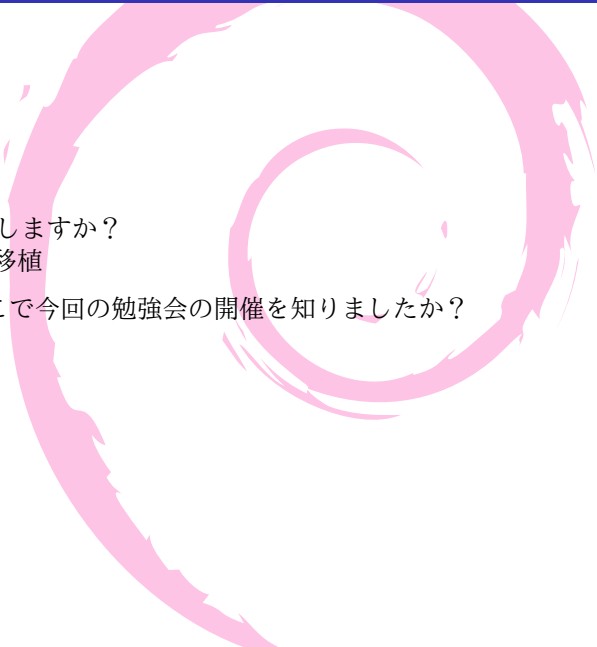
- 注意事項
 - 写真はセミナー
ルーム内のみ可
です。
 - 出入りは自由でな
いので、もし外出
したい方は、野島
まで一声ください
ませ。
- 事前課題発表
- 最近あった Debian 関
連のイベント報告
 - 第 126 回 東京エリ
ア Debian 勉強会
- Debian Trivia Quiz
- Debian と脆弱性対応
のあれこれをまとめて
みた
- 今後のイベント
- 今日の宴会場所

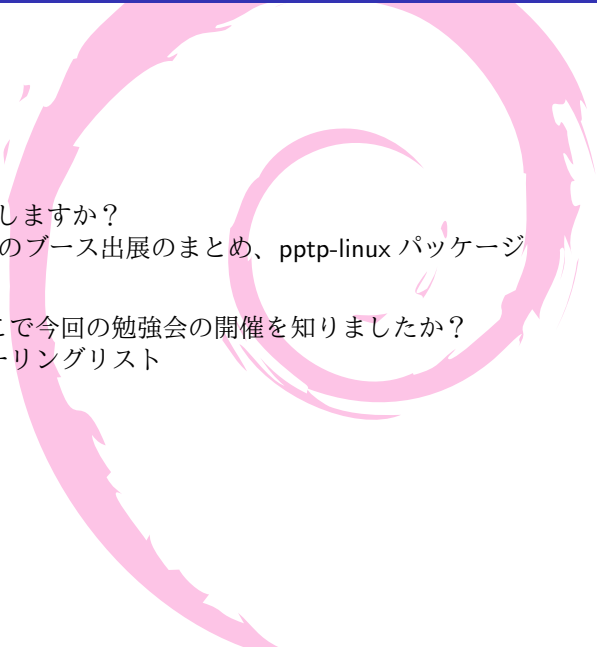


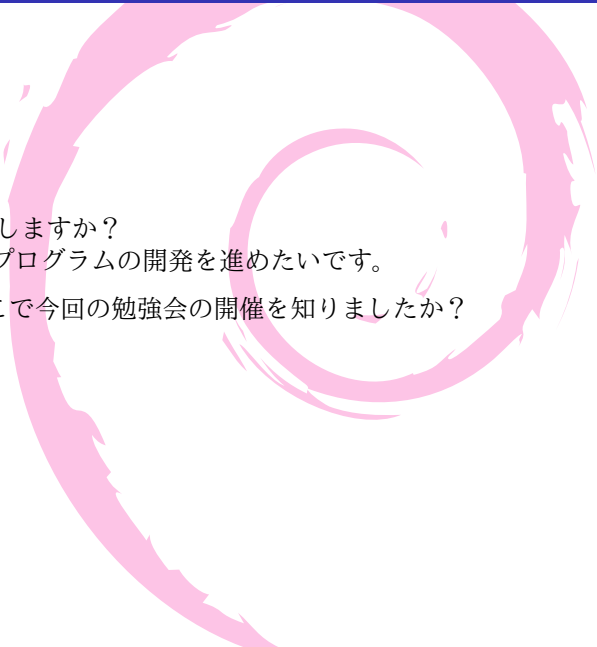
事前課題

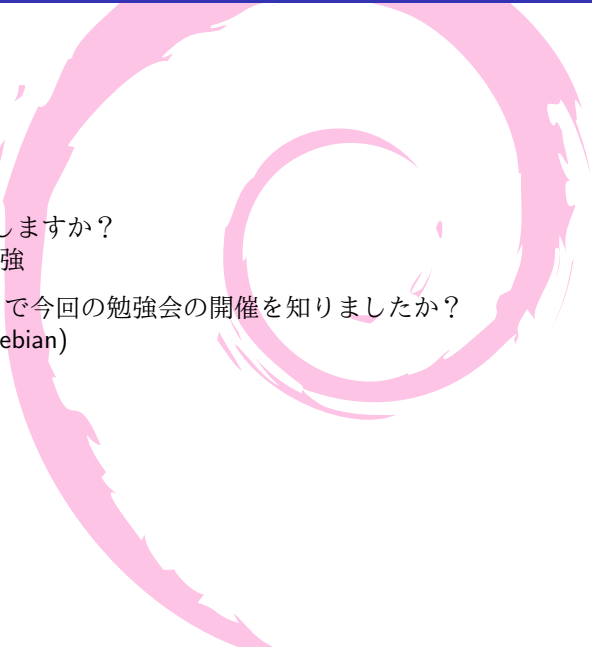
- 
- ① Q.hack time に何をしますか？
A. Nook HD+をそろそろ debian を動かす件かな？
 - ② (オプション)Q. 何について聞きたい／参加者と話をしたいですか？
A. Debian! Debian! Debian!

- 
- ① 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 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 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 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 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)



イベント報
告

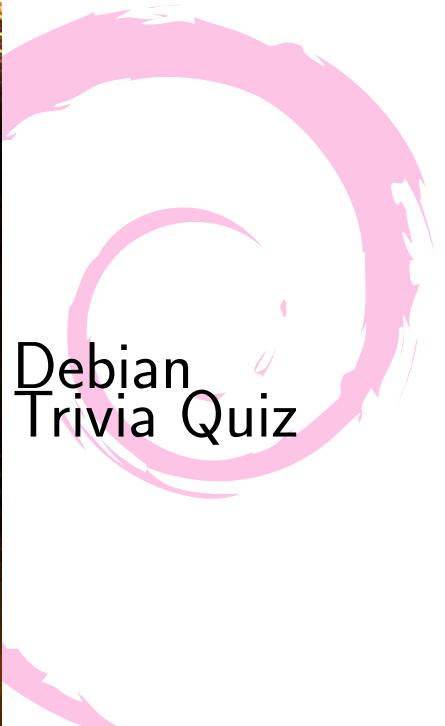
第126回東京エリア Debian 勉強会

- 場所はスクウェア・エニックスさんのセミナー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。

第126回東京エリア Debian 勉強会(つづき)

セミナーは野首さん（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の良いと思いました。



Debian Trivia Quiz




Debian Trivia Quiz

Debian の常識、もちろん知ってますよね？ 知らないなんて
恥ずかしくて、知らないとは言えないあんなことやこんな
こと、みんなで確認してみましよう。

今回の出題範囲は

`debian-devel-announce@lists.debian.org`,
`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/



C 2015/6/

答えは:






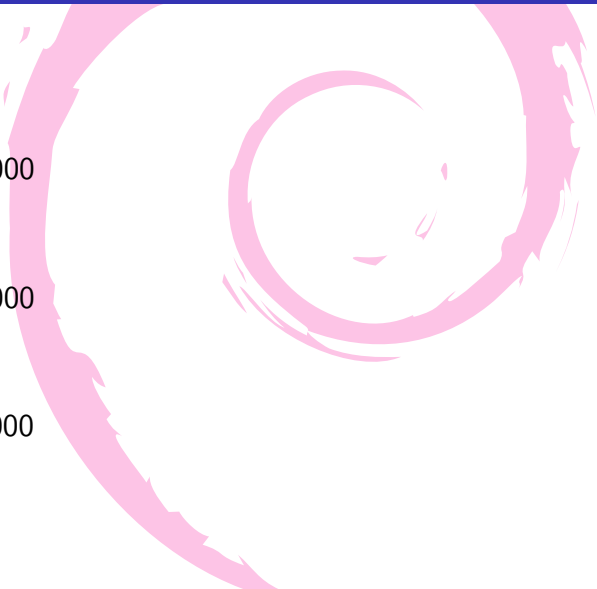
A

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？




解説：いくつかの脆弱性対策や、バグフィックスが行われたパッケージが取り込まれました。Debian 8(Jessie)をインストールしたばかりの人は、早速アップグレードしましょう！

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

答えは:






B

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？



解説：遂に22,000を超えたそうです。バイナリパッケージ
の数は45,542との事。益々増えていくようです。

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

問題3. AutomaticDebugPackages の提案とは何？

答えは:

-  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...にする
-  C `-dbg`め、`.ddeb`



C

問題3. AutomaticDebugPackages の提案とは何？

解説：今まで、デバッグシンボルは`-dbg`パッケージで配布されてきました。しかしながら、こちらの`-dbg`パッケージは他のデバッグとは何ら関係のないパッケージと一緒にmirrorされるため、`-dbg`パッケージの利用者がとても少ないにもかかわらず、mirror先の資源をその分消費してしまいます。今回の提案は、デバッグシンボル`.ddeb`というパッケージにしてしまい、こちらのパッケージについてはmirror先も減らす（しない？）という事を検討するものです。



Debian と脆弱性対応の
あれこれを
まとめてみた

はじめに

Debian で行われている脆弱性対応の話を紹介します。

- いつかまとめてみたかったのは秘密...
- 本発表はとあるセキュリティの勉強会で使った資料です。悪しからず。

自己紹介

野島 貴英

東京エリア Debian 勉強会の中の人。毎月 1 回ですが、勉強会やっています。興味ありましたら、是非是非ドゾー。

<http://debianjp.comnpass.com/>

<http://tokyodebian.alioth.debian.org/>

<http://www.debian.or.jp>

Debian とは

- Debian は Debian 社会契約 (*1) を理念として開発されている OS ディストリビューションの1つ。
- 純粹にコミュニティ活動と多数のボランティアにより、開発が継続しているのが特徴。また、Debian に関する重要な事柄が（リーダー就任すらも）Debian Project 関係者らの投票で決められたりする。とにかくオープン。
- 収録されているプログラムの元となるソースパッケージ数は 22,000 パッケージを超えた。

(*1) https://www.debian.org/social_contract

ちょっと用語：Debian パッケージって？

- Debian を構成するアプリケーションのデータや実行バイナリをまとめたもの (.deb ファイル。)
- ソースコードをまとめたソースパッケージもある (.tar.gz, .dsc ファイル。)

Debian のセキュリティチーム

- 連絡先 : security@debian.org または team@security.debian.org
- 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。

脆弱性に関する ML

- 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/`

例外もあるよ！

Debian パッケージのアーカイブエリアとして、
main, contrib, non-free の3つがある。

contrib と non-free に属する脆弱性
対応は基本無し(ズガン！)

例外もあるよ！(つづき)

理由：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で、勝手に直すことが許諾されていない場合があるため。

contrib と non-free であっても、ライセンス上、直しても良いものについては、通常通りセキュリティチームにて対応が図られる。

脆弱性に関する対応の流れ

Debian ユーザあるいは Debian の関係者にかかわらず、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 する。

PAT2: 既知でない場合は、そつと security@debian.org
または team@security.debian.org にメールで連絡
(英文) し、あとは指示に従う。

なお、脆弱性対策パッチをうっかり書いたのであれば、報告の際にパッチも一緒に送ると喜ばれる。

脆弱性に関する対応の流れ(つづき)

- 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）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る。
- 既知の脆弱性については、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る。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。

参考：BTSするって？

Debian パッケージのバグ追跡ツールである、<https://bugs.debian.org> に登録されるようなバグレポートを送る事。

特定のフォーマットで記載したメールでバグレポート（英語）を送ることにより、登録される。Debian のユーザであれば誰でもレポートは送ることができる。

脆弱性対応状況の確認方法

- ① セキュリティ観点のもの
 - <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。
- ② QA 観点のもの
 - <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る。
- ③ BTS したもの
 - <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。

その他トピック

昨今の Debian のセキュリティに関するトピックをいくつか。ここでは、

- Hardening
- Debian パッケージ済みの脆弱性静的解析ツール群紹介
- lintian
- systemd
- Reproducible Builds
- LTS(Long Term Support)
- debian-security-support パッケージ

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パッケージを作る事。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、
"-fstack-protector-strong -Wformat -Werror=format-security -D_FORTIFY_SOURCE=2"
となる。

Debian パッケージ済みの脆弱性静的解析ツール 群紹介

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する。
2	rats	C, Perl, PHP, Python のコード上問題の起きそうな部分を指摘する。
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する。

Table: 脆弱性静的解析ツール

- 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。
- 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る。

昨今搭載された例：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。

外部リンクあったら、ブラウザで HTML ファイル開いた瞬間に良からぬサイトへアクセスしちゃったとかあるとマズイですよ...

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る。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。

良い文章：

「Security Features in systemd」

<http://0pointer.net/public/systemd-nluug-2014.pdf>

Reproducible Builds

簡単に言うと、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 パッケージと照合する試み。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。Debian の他にも、Fedora/OpenSUSE/NixOS でも行われている。

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/>

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。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するというもの。

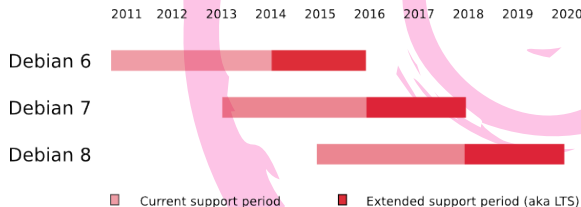


Figure: LTS のサポート期間

LTS(Long Time Support) つづき

LTSは無料で利用できる一方、有償サポート契約も用意されている。有償サポート契約を Freexian 社と行くと、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に関して、要望が通りやすくなるという特典がある。日本の会社様にての契約締結実績は GREE 社のみ。

詳しくは：

「Debian Long Term Support」

https:

[//www.freexian.com/en/services/debian-lts.html](https://www.freexian.com/en/services/debian-lts.html)

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った。

debian-security-support パッケージ (つづき)

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、各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るパッケージ名を照合し、制限があるパッケージが見つかった場合は警告を出すという動作。LTS の元では、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に便利。

おわりに

Debian のコミュニティは、Linux、OSS にまつわる様々な問題点や課題を、コミュニティの力を結集して日夜解決していくのがミッションであり、参加の醍醐味です。日夜、技術的課題、セキュリティ問題も含め、解決・考察し甲斐のある課題が、次から次へと生まれています。

是非、Debian へのご参加お待ちしております!!



今後のイベント

今後のイベント

- 関西エリア Debian 勉強会
- 東京エリア Debian 勉強会 (7/某日)



今日の宴会
場所

今日の宴会場所

未定

