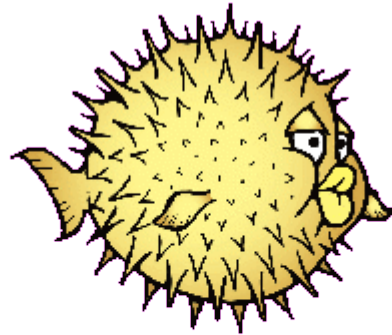


あなたの知らないOpenBSD

“Sending script kiddies to /dev/null since 1995”

Tomoyuki Sakurai
<cherry@trombik.org>



OpenBSD

このセミナーのポリシー

- 質問は随時受け付けます
- 長くなりそうな質問には終わった後で答えます

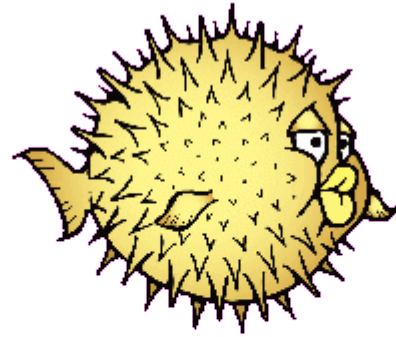


歴史

- NetBSDからfork
 - 理由はよくあるけんか [1]
- イラク戦争反対でDoDとけんか
 - 資金援助打ち切り [2]
- セキュリティといえばOpenBSD
 - デフォルトインストールで過去10年間に存在したりリモートからの脆弱性は2つ
- すばらしいサブプロジェクト
 - OpenSSH, OpenNTPD, OpenBGPD, OpenCVS...



FAQ嫁



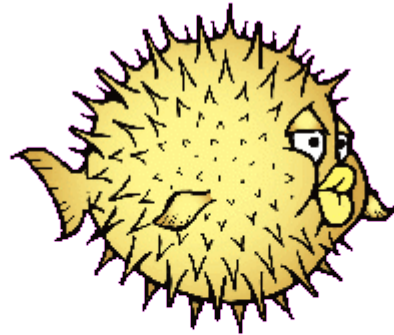
***Open*BSD**

FAQ

- Apache 2.xはbase systemに入りません
- 「動けばいいじゃないか」は通用しません
- standard != open
- kernelの再構築はおすすめしません
- Sendmailはパッチを受け入れるのでいいひとたちです
- ユーザビリティが良くなければ意味がありません



好きなものと嫌いなもの



***Open*BSD**

理念

■ 自由、機能性、セキュリティ

- “Free as in air” [3]
- BSDライセンス命
 - kernelはBSD only、その他はやむを得ない場合にのみGPL可
- 必要であればスクラッチからコードを書くぜ

■ セキュリティと監査

- 最初から正しいコーディング
- バグを見つけたら、同様のパターンのバグを探し、修正

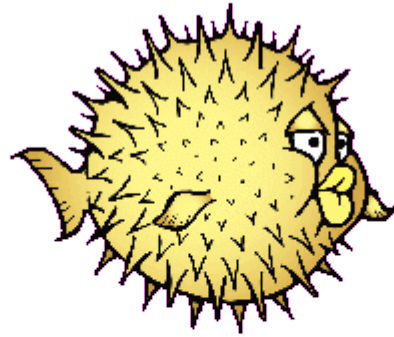


天敵

- ドキュメントを公開しないベンダ
 - Intel (wireless)、Broadcom (wireless)
 - Adaptec (aac(4) [4])
- ライセンス
 - ipfilter (packet filterなしでリリース、pfの誕生)
 - Cisco (VRRP、CARPの誕生)
 - DJB (portsのライセンス見直し、qmailやdjbdnsの削除 [5])
 - RMS (悪魔呼ばわり)



Security



***Open*BSD**

セキュリティ

■ コード監査

- バグの修正がセキュリティの向上に
- 誤用されやすい関数は書き替え (strcpy, strcat, [6])
- 「OpenBSDではその問題は10年前に修正されています」
CVE-2007-2926 [7]

■ 乱数の使用

- メモリ、ネットワークスタックなど考えられるものすべて

■ 権限の分離

- 最小特権の原則
- 特権が必要なコードを最小限に



セキュリティ

- マニュアルには豊富な使用例
 - システムコールからコマンドまで
 - よろしくないドキュメントはバグとみなされる
- 先進的なセキュリティ
 - W^X、メモリアドレスの保護 (Windows Vistaにも採用 [8])
- 開発者に安全なプラットフォームを提供 [9]
 - 思い込みで書かれたコードは動かない
 - バグを見つけやすい



セキュリティ

- 機能の追加だけが進歩ではない
- 継続的なrefactoring [10]
 - コードが増えればbugが含まれる可能性も増える
 - 肥大したコードは監査しにくい
 - 特権が必要なコードを追い出す

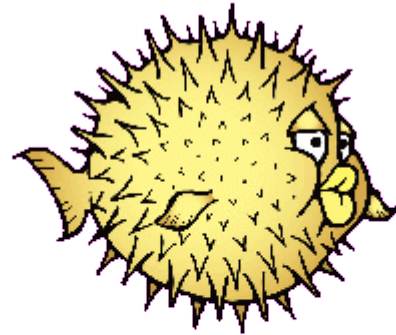


contrib

- base system + ports = OpenBSD
 - kernel + user land + contrib = base system
- httpd(8)にはpatchがたくさん
 - 1.x-based、defaultでchroot
 - もはや別のツリー
 - Apache License Version 2は許容できない
- named(8)にもpatch
 - CVE-2007-2926 [7]
- gcc(1)からpccへ移行するかも?



優れたボスには優れた部下が



***Open*BSD**

開発体制

- 開発者数は約90人
- 遅れないリリース
 - CDを注文するとリリースの1ヶ月前に届きます
- ゆっくりと、着実に進化
- 年1回Hackathonをカナダのカルガリーで開催
 - ホテルで開発合宿
 - スケジュールなし、好きな時にhack
 - 終わったらみんなでトレッキング



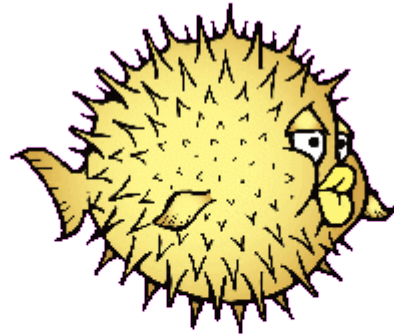
名物男

その名はTheo de Raadt

- OpenBSDの皇帝
 - バス問題には「シラネーヨ」
 - 最近、考え方が変わったという噂も
- OSの設計して十余年
 - マネージメントから実装まで
 - 「技術的なことでヤツと議論しても勝てません」
- メールとその実像の解離っぷりは異常
- 開発者の団結力の高さは異常
 - 部下思いの頼れるボス



優れた機能も使いにくければ
意味がない



***Open*BSD**

ユーザビリティ

- スケジュールに沿ったリリース
 - アップデート計画が立てやすい
- 安定したパッケージシステム
 - portsとbase systemは同時にリリース
 - stableには脆弱性の修正と重要なbug fixだけ
- 1つのプロジェクトによって開発される完全なOS



ユーザに優しく

- ntpdとOpenNTPD
 - man ntpd.conf | wc -w = 483
 - man ntp.conf | wc -w = 13150
- iptablesとpf
- IPsec [11]



ntpd.conf(5)

```
# ntp client
servers pool.ntp.org

# ntp server
listen on *
servers ntp.example.org
```



pf.conf(5)

```
pass in on $ext_if proto udp \  
    from any to $dns_servers port domain keep state  
pass in on $ext_if proto tcp \  
    from any to $dns_servers port domain \  
    flags S/SA modulate state  
pass in on $ext_if proto tcp \  
    from any to $web_servers port { http, https } \  
    flags S/SA modulate state
```



ipsec.conf(5)

```
ike esp from 10.1.1.0/24 to 10.1.2.0/24 \  
peer 192.168.3.2 \  
srcid me.example.org dstid his.example.org
```

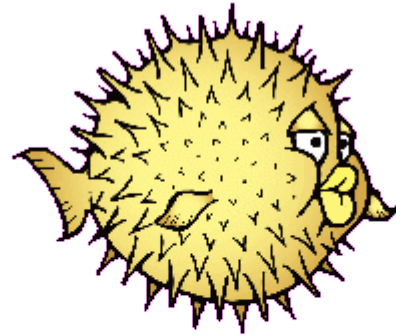


日本語対応

- かつては鬼門だった
 - cannaとかwnnとか
- 4.1から大幅に改善
 - uim, anthy
 - でもまだ問題あり
- OpenOffice.orgも
- 「日本人がメンテナンスしてよ」



Someone you can trust



***Open*BSD**

高い技術力

■ 数々の独自実装

- Open*(OpenSSLは違います)

■ 頭に来たらプロトコルだってスクラッチから書くぜ

- CARP

■ reverse engineering 上等

- wirelessデバイスのサポート状況は世界一
- RAID management interface, bioctl(8)



ユニークな機能

- CARPによるHA
 - VRRPはライセンスに問題アリ
 - virtual IP basedのactive - stanby構成
- defaultでロードバランサーが付いてくる唯一のOS
 - hoststated(8)
 - L3とL7(HTTP)
- defaultでBGPも話せます
 - OpenBGPD、OpenOSPF

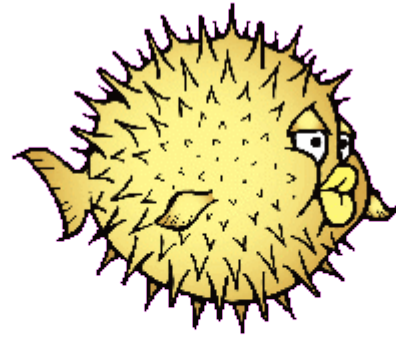


改善点

- rcが古い
 - rc.subr採用してほしい
- WEPしか使えない
 - WPAとか使いたい「IPSec使え」
 - work in progress :)
- mergemasterをbaseに入れてほしい
- FLAVORを一ヶ所で管理したい
- PORTDIR_OVERLAYが欲しい
- openbsd-update欲しい



大人の事情



OpenBSD

OpenBSD Support Japan Inc.

- 世界で唯一のofficial OpenBSDサポートを提供
- 売上げの一部はOpenBSDプロジェクトへ
- 社員の半数以上が開発者
- セキュリティ、システム管理からIPv6まで
- PACSEC(2007/11/29, 30) officialスポンサー
- <http://www.openbsd-support.com/>



Question?



御静聴ありがとうございました



References

- [1] NetBSDからforkするまでのやりとり
- [2] DARPA funding cancellation
- [3] OpenBSD: Free As In Air
- [4] Adaptec AAC raid support
- [5] Re: Why were all DJB's ports removed? No more qmail?
- [6] strcpy and strcat
- [7] OpenBSD & BIND 9 cache poisoning
- [8] Exploit Mitigation Techniques
- [9] OpenBSD as a Development Platform
- [10] Security measures in OpenSSH
- [11] Recent Improvements in OpenBSD's IPsec Support



If time permits...

■ portsはFreeBSD-based

- one ports tree per a release
- アップデートは年に2回(release)

■ FLAVORS

- FreeBSDのOPTIONSみたいなもの
- screen-<version>-static

■ MULTI_PACKAGES

- database/mysqlならmysql-client-<version>

