



オープンソースカンファレンス 2017 Tokyo/Spring

2年半ぶりのリリース！
xrdp v0.9.1とLinuxディストリビューションの
連携と新体制

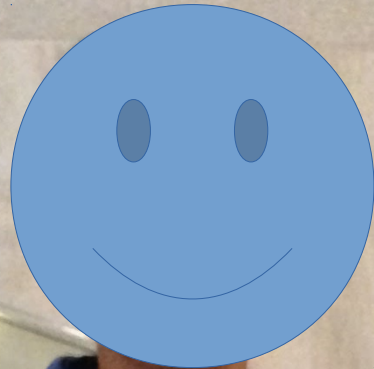
日本xrdpユーザ会 / xrdp project
2017年3月11日



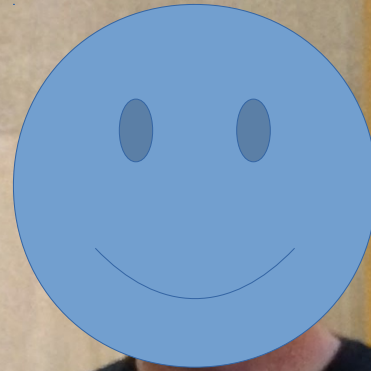


自己紹介





metalefty



Jay Sorg

Sep 28, 2015 @San Jose, CA



Contributors

Traffic

Commits

Code frequency

Punch card

Network

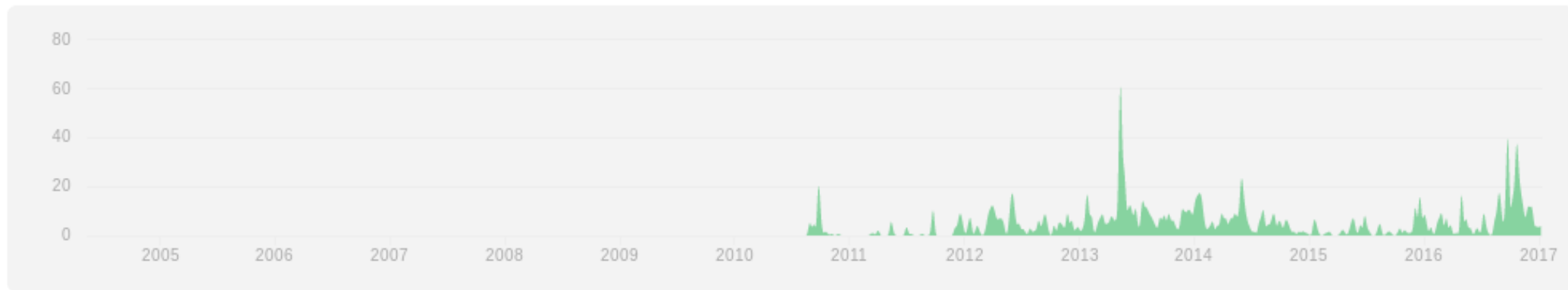
Members

Dependents

Jul 2004 – Mar 2, 2017

Contributions: **Commits** ▾

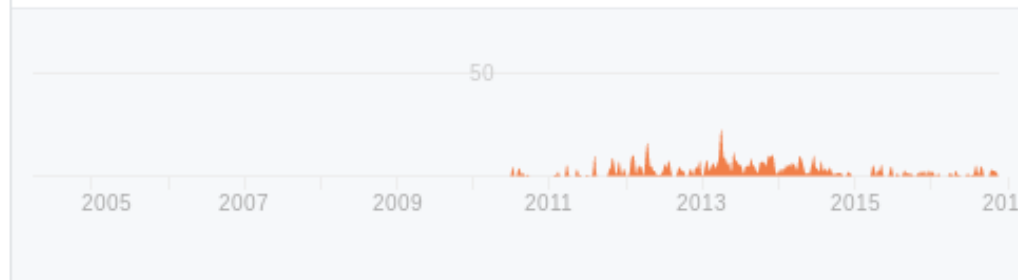
Contributions to devel, excluding merge commits



jsorg71

#1

902 commits / 100,568 ++ / 46,126 --



proski

#2

259 commits / 6,212 ++ / 10,603 --



speidy

#3

123 commits / 6,104 ++ / 7,962 --



metaleft

#4

120 commits / 19,659 ++ / 17,025 --





自己紹介

- xrdp developer
 - 非ASCII文字圏では唯一のメンバー
- 日本xrdpユーザ会 発起人
 - 2013年設立
 - ユーザとしては2009年から
- シンククライアントだいすき
 - おーぷんここんは対極の存在のお友達





自己紹介

- 日本語/東アジア言語固有のバグを修正
 - メインの開発者が英語圏
 - 非英語圏でもASCII文字圏が多い
 - 最近なくなってきた
- TLS/SSL関連の修正・機能追加
- パッチのあるものはレビューします
- 少なくとも再現できることが必要





自己紹介

- ユーザ会なのに気がついたら開発者になった
- 最近ユーザ向け情報を発信できてないかも
- どういう情報が欲しいですか？
 - アンケートに回答お願いします
 - 次回移行の参考にします





こういう話の方がいいですか？

オープンソースカンファレンス 2017 Tokyo/Spring

懇親会LT

Microsoft Remote Desktop for Mac の
キー配列について

日本xrdpユーザ会
2017年3月10日





今日話すこと

- 2年半ぶりのリリース
 - v0.9.1 リリースまでのいきさつ
- リリースサイクルの見直し
- Linux distroとの連携
- 次期リリースv0.9.2のトピック





xrdp v0.9.1 リリース！

- v0.9.1 - 2016年12月23日
 - V0.6.2 - 2016年10月4日
 - v0.8.0 - 2014年7月24日 ←ここから数えて
- v0.9.0 はスキップ
 - リリース前の開発版にリリースバージョンをつけてパッケージしてしまったFというdistroがある
 - 0.9.0.betaYYYYmmdd みたいなバージョンにすべきだった
 - 混乱を避けるためスキップ





なぜこんなに空いてしまったのか

- 開発者のSAGA
 - 最前線をぐいぐい進めることにしか興味がない
 - マイルストーンを置いてこなかった
 - リソース不足
- ユーザはどれを使えばいいのかわからない
- こんなんじゃないだめだとよずっと言ってきた
- リリースしてくれというissueが複数立つ





リリースは積年の課題だった

- v0.8.0移行まともにリリースされていない
- リリースされないからdistroに収録されない
- distroに収録されないからテストされない





Debianからの提案 (2016年10月)

- Dominik George (from Debian Education?)
 - Debian 9 (stretch)に最新版xrdpを入れたい
 - そのためには明確なリリースが必要
 - リリースのための“xrdp hackathon”をやらない？
 - Debianの締切(soft-freeze)は2017年1月5日
 - Debian側の作業も含めると年内にはリリースしなければならない





Dominikと水面下でやりとり

- 私
 - “xrdp hackathon” (・∀・)イネ!!
 - 他のメンバー次第だけどリリースする方向になるようxrdpチームに言ってみるよ!
 - OSCでも安定版リリースが欲しいという意見を各所から頂く
 - 日本の企業ユーザもリリースして欲しがっている
 - 少し誇張気味に伝える(・ω<)





xrdpチームが重い腰を上げる

- これまで
 - xrdp開発チームに入る前から私1人が口うるさく「リリース！リリース！」
 - リリースの必要性はわかってる、でもねえ…
- だんだんこうなってきた
 - 外野の味方が増えてきた
 - どれを使ったらいいのかわからないユーザ
 - distroのパッケージメンテナにつつかれる





リリース日の決定

- 締切駆動開発で行こう
- Debianのリポジトリに入って困ることはない
 - ぜひ入れよう
 - Debian側の締切に合わせてリリース日を設定
- 2016年の最終週の1つ前の週
 - 12月17日～24日のどこか





Debianに入ることの効果

- 多数のDebianベースのdistro
 - Ubuntu
 - Linux Mint
 - Raspbian
- Debian 9のリポジトリに入ること
これらのdistroでもaptで入れるだけになる





新しいリリースサイクル

- Time-based release (quarterly)
 - 年に最低4回リリースする(3, 6, 9, 12月)
 - 時間がきたら致命的なバグがない限りリリース
 - 残っているバグは次までに直すか臨時リリースする
 - バージョンに日付は含めない (17.03等)
 - 安定してリリースするものがなくなったときに古く見える
 - 何年も新版がリリースされてないけど時代遅れではないソフトウェア、ありますよね？

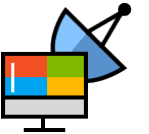




年末まで怒涛の勢いで開発

- 開発メンバーが世界各地に分散
 - カリフォルニア (UTC+17)
 - 日本 (UTC+9)
 - イスラエル (UTC+2)
 - ドイツ (UTC+1) – Debian パッケージメンテナ
 - ブラジル (UTC-3)







— 人 人 人 人 人 人 人 人 人 —
> 時差が <
> ちょうどいい <
— Y ^ Y ^ Y ^ Y ^ Y ^ Y ^ Y ^ Y ^ Y —





グローバル開発

- ちょうどいい時差のおかげでいい感じに進む
 - 同時に意見交換するには向かないが…
- イスラエル・日本・カリフォルニアの3チーム
 - チームといっても各1人
 - ドイツのDebianチームがテストしてくれる
- という流れでリリース





そしてリリース

- 2016年12月23日 xrdp v0.9.1 リリース
- Debian Stretch "Soft" freeze に間に合う
- Debian 9 "Stretch"はもうすぐ？
 - apt install xrdp ですぐ使えるはず
 - TLSを使う場合はxrdpユーザをssl-certグループに
usermod -G ssl-cert xrdp





Distroとの連携

- Debian
 - xrdp team と Debian Remote Maintainers が連携
- Fedora
- FreeBSD
 - xrdp 開発メンバーがパッケージメンテナ
- その他のdistro





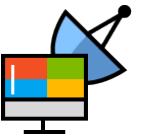
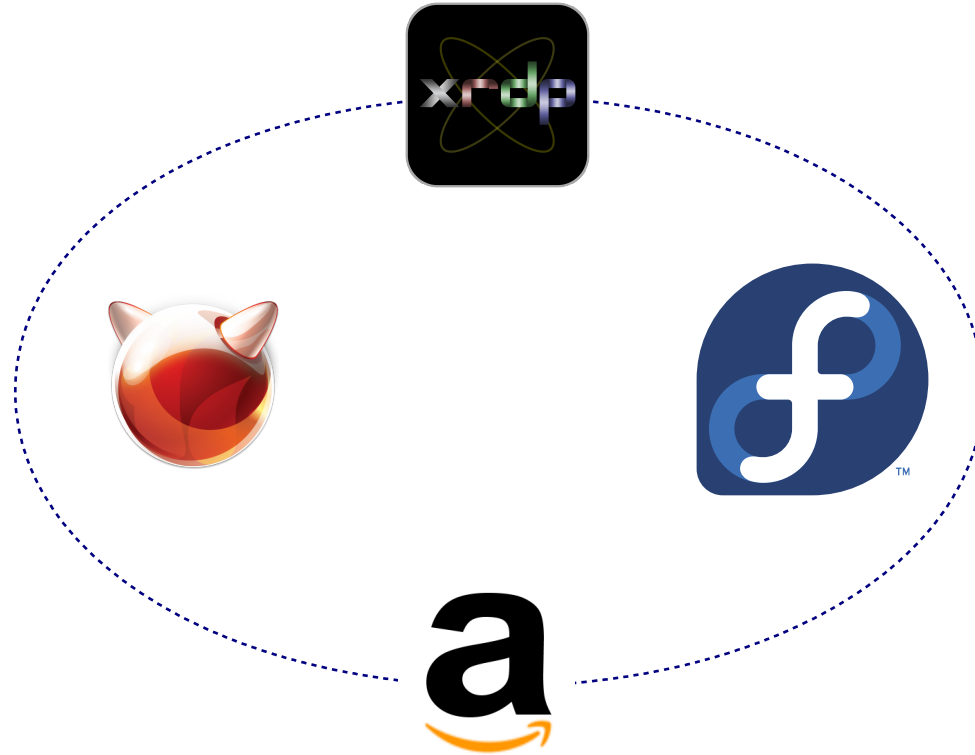
今後のリリース

- Quarterly (四半期ごと)のリリース
- 2017年3月
(そう、今月！)
- 3月30日を予定 (年度末…)
- それ以後も定期的にリリースしていきます



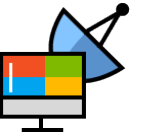


相関図





v0.9.1 から v0.9.2 で何が変わったか





v0.9.2 での変更

- 全体的なお掃除が多い
 - インデントやコーディング規約に沿うよう修正
 - コンパイル時の warning 潰し,マジックナンバーの定数化
 - メモリリーク修正
- 日本語キーボード検出のリグレッション修正
- Travis によるCIの強化
- SSL/TLS関連の修正





v0.9.2 での変更

- Android版クライアントで接続できない問題
 - v0.9.1 で修正済み(オプション扱い)
 - v0.9.2 でデフォルトに





v0.9.2 での変更

- SSL/TLS 関連の修正
 - OpenSSL 0.9.8より前のサポートを廃止
 - 使用中のTLS, cipher suite をログに記録
 - SSL/TLS ver を指定可能になった
 - TLS使用時にCPU使用率が高くなるバグを修正





使用中のTLS, cipher suiteの出力

[20170131-11:03:00] [INFO] TLS connection established from ::ffff:192.168.69.1 port 55920: **TLSv1.2** with cipher **AES256-GCM-SHA384** (一例)

- xrdpとクライアントの間の暗号化情報
- 現時点では安全とされている
 - TLSv1.2
 - AES256-GCM-SHA384





クライアントとTLSの対応一覧

	TLS version	Cipher Suite
Windows 7 (mstsc.exe)	1.0	AES128-SHA
Windows 10 (mstsc.exe)	1.2	AES256-GCM-SHA384
rdesktop 1.8.3	1.0	AES256-SHA
FreeRDP 1.2.0	1.0	AES256-SHA
MS Remote Desktop		
for Mac OS X 8.0.34	1.2	AES256-GCM-SHA256
for iOS 8.1.26	1.2	AES256-GCM-SHA256
for Android 8.1.37.135	1.2	AES256-GCM-SHA256
RDC for Mac 2.1.0	1.0	DES-CBC3-SHA

※ 最も優先して使われたものだけを記載しています





SSL/TLSバージョンの指定機能

- SSLv3からTLSv1.3まで任意で使用可能
 - SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
 - SSLv2は使用不可 (hard-coded)
- `ssl_protocols` で指定 (xrdp.ini)
 - カンマまたはスペース区切り
 - 例: `ssl_protocols=TLSv1.2, TLSv1.3`





SSL/TLSバージョンの指定機能

- TLS cipher suite の指定と合わせてより強固なセキュリティが実現可能になった
 - PCI DSS v3.2などのセキュリティ基準に準拠可
 - 全てのSSLとTLSv1.0を無効化
 - 新規システムはTLSv1.1以上が必須
 - 将来TLSv1.2以上に引き上げられる可能性もある
- ※クレジットカード業界のセキュリティ基準





TLS cipher suite の指定

- これはv0.9.1からの機能
- xrdp.ini の `tls_ciphers` で指定
 - 今のところデフォルトはコメントアウト
 - 解除しておきましょう
 - 最低でもHIGH以上
- `openssl ciphers` コマンドに指定可能なもの



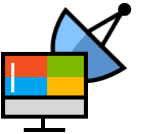


OSSプロジェクトから見る upstreamとdistroのつながり





- オープンソース
- エンドユーザが使うのはdistroに収録されるパッケージであることが多い
- aptでインストールするだけ
 - 布教の大いなるきっかけ





開発者サイドでできること

- distroのパッケージメンテナとは仲良くする
- メンテナはそのソフトウェアのユーザでもある
 - 少なくとも1人はユーザがいるという励み
- 主要distroのパッケージバグトラッカは追う
 - ユーザ視点の報告が多数
 - バグでないものもあるが開発の参考になる





Debian bug #856436

- security_layer=tls と設定すると接続できない
- 証明書ファイルにパーミッションがないのが原因
- Debian的には必要に応じてユーザを ssl-certグループに追加するのが習わし
- パッケージのバグでもxrdpのバグでもないという結論になった





Debian bug #856436

- 証明書ファイルが読み込めなかったときにエラーメッセージが出ないのは不親切だよね
- xrdp側でもうちょっと親切になるようにしよう

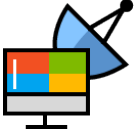




仲良くしておくといいいこと

- アプリケーション開発者は各distro固有のお作法に必ずしも詳しいわけではない
- distro固有のお作法部分はやってくれる
- アプリケーションとdistroのどちらで対応すべき問題か切り分けてくれる





Gentoo, Arch Linux 方面の人募集
仲良くしましょう

