オープンソースカンファレンス 2016 Tokyo/Fall

xrdpの最新動向と新機能

#xrdp_jp #osc16tk

日本xrdpユーザ会

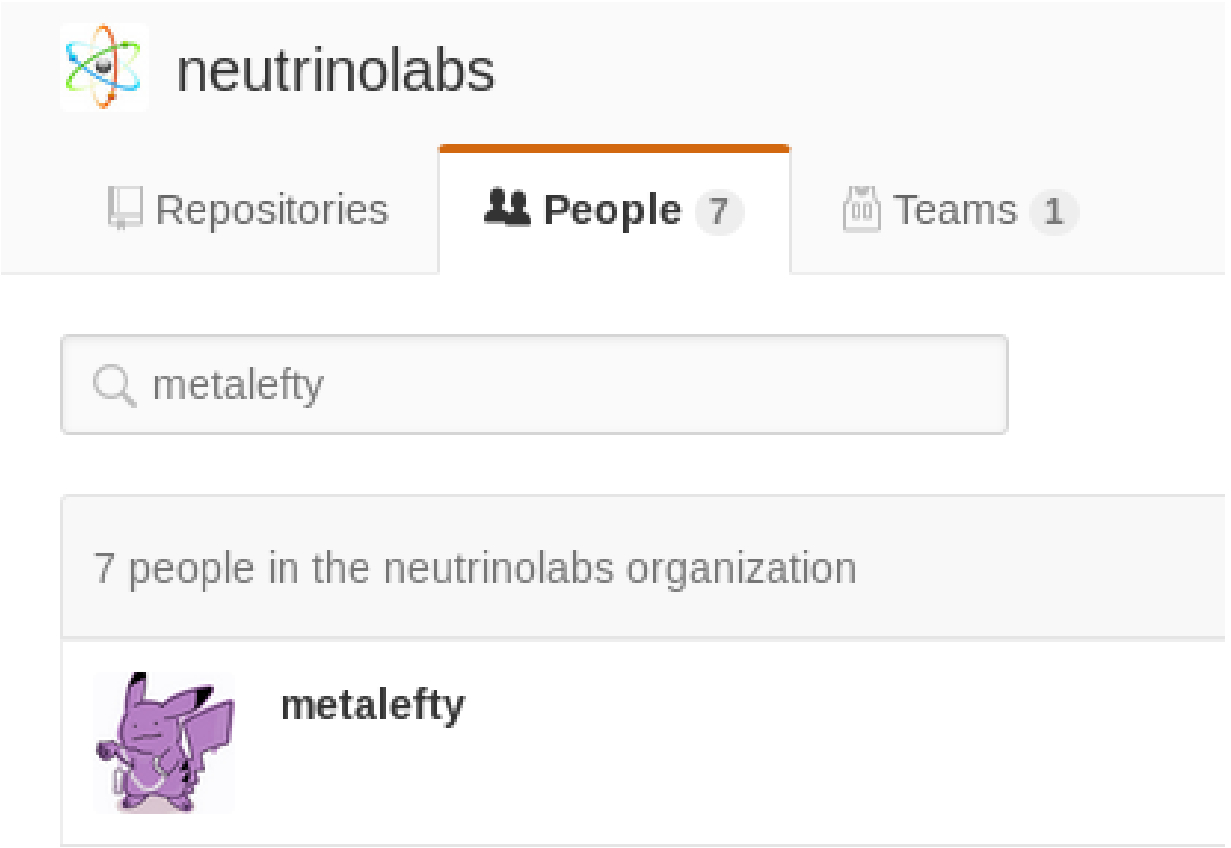
2016年11月6日

突然ですがご報告

中の人になりました


めた | CBA-NCEC
@metalefty
xrdp開発チームに入ったらしいです。中の人を名乗れるようになった。 #xrdp_jp
Search GitHub
jsorg71 added metalefty to neutrinolabs/xrdp 33 seconds ago
4
リツイート
12
いいね
19:03 - 2016年6月29日
4
12

organizationのメンバー



何が変わったかというと

- neutrinolabs のメンバーになった
- リポジトリへのpush権限を得た
- issueを操作する権限を得た
- 中の人を名乗れるようになった

最近やっていること

- Issue の整理
- IPv6 系のバグ修正
- 使用中の暗号をログに出力
- プロトコル方面は苦手です
- Debian チームとの連携

今後もよろしくお願いします

今日話すこと

- 自己紹介
- 日本xrdpユーザ会について
- xrdp 開発の最近のトピック
  - MP3 サポート
  - SSL 3.0 の無効化
  - TLS cipher suite の選択
  - Android版クライアント
- Debianにxorgxrdpが来た話

自己紹介

- 日本xrdpユーザ会発起人
- 2009年からxrdpのユーザ
- xrdp開発者 ←NEW!!
  - 開発自体は以前からやっていた
  - 中の人になりました
  - 非ASCII文字圏では唯一のプロジェクトメンバー
  - PRを送る日本人は他にもいます

自己紹介

- 日本語/東アジア言語環境固有のバグ
  - メインの開発者が英語圏
  - 非英語圏であってもASCII文字圏が多い
  - テストされにくい
- 声を上げたほうが優先度が高くなります
- パッチがあるものは後押しします
- 少なくとも再現できることが必要

日本xrdpユーザ会

- 2013年10月19日に設立 @2013 Fukuoka LT
- xrdp の開発者やユーザ、各distroへの移植者・パッケージャが集まるゆるい会(を目指す)
- OSCに出展するときの肩書の役割も
- 成果物
  - X11RDP-RH-Matic
  - X11RDP-o-Matic


metalefty
Jay Sorg
Sep 28, 2015 @San Jose, CA

日本xrdpユーザ会

- 開発者 Jay Sorg に会ったことがある
  - だからなんだ
  - 多少は偉そうにできる
- ユーザ会の肩書で発表したい場合
  - ご相談ください
  - 内容のチェックをする場合があります

日本xrdpユーザ会

- ゆるい会なので会員も未定義
- 1人ユーザ会的性質もある
- MLのメンバー数を基準とすると
  - 20人 (2016年2月22日現在)
  - 30人 (2016年8月30日現在)
- ユーザ会発のbug fixは
  - 過去2件 (ありがとうございます)

xrdpの最近のトピック

中の人になりました


めた | CBA-NCEC
@metalefty
xrdp開発チームに入ったらしいです。中の人を名乗れるようになった。 #xrdp_jp
Search GitHub
jsorg71 added metalefty to neutrinolabs/xrdp 33 seconds ago
4
リツイート
12
いいね
19:03 - 2016年6月29日
4
12

Debian sid に最新版が入った

[ソース: xrdp]

[wheezy][jessie][jessie-backports][stretch][sid]

パッケージ: xrdp (0.9.0~20160601+git703fedd-3 など)

Remote Desktop Protocol (RDP) server

xrdp offers a graphical login to a remote client using RDP (the Remote Desktop Protocol). xrdp can connect to a locally created X.org session with the xorgxrdp drivers, to a VNC X11 server, and forward to another RDP server.

xrdp accepts connections from freerdp, rdesktop, and the built-in terminal server / remote desktop clients of Microsoft Windows operating systems. In the xorgxrdp (which replaces X11RDP) and VNC modes, it provides a fully functional Linux terminal server, offering an X-Window desktop to the user. In the RDP or VNC forwarding mode, any sort of desktop can be used.

xrdp に関するリンク

Debian の資源:

- バグ報告
- 開発者情報 (PTS)
- Debian での変更履歴
- 著作権ファイル
- Debian パッチ追跡システム

xrdp ソースパッケージをダウンロード:

xorgxrdp も入った

[ソース: xrdp]

[jessie-backports][stretch][sid]

パッケージ: xorgxrdp (0.9.0~20160601+git703fedd-3)

Remote Desktop Protocol (RDP) modules for X.org

xorgxrdp is a set of drivers (screen device, keyboard, and mouse) for X.org enabling use through an RDP session with xrdp. For full operation, most standard X11 fonts and tools need to be installed; the Recommended xorg metapackage is a superset of what's actually needed but will do.

その他の xorgxrdp 関連パッケージ

● 依存 ■ 推奨 ◆ 提案 ▲ enhances

- **dep: libc6 (>= 2.15) [alpha, arm64, ppc64el, sh4, x32 以外]**
  GNU C ライブラリ: 共有ライブラリ

xorgxrdp に関するリンク

No screenshot available. Sorry.

Debian の資源:

- バグ報告
- 開発者情報 (PTS)
- Debian での変更履歴
- 著作権ファイル
- Debian パッチ追跡システム

xrdp ソースパッケージをダウンロード:

- [xrdp_0.9.0~20160601+git703fedd-

Debian sid が開発版をパッケージ

- そのうち Ubuntu にも降ってくるかも？
- 公式リリースをしないせい
  - ごめんなさい
  - 最後のリリースが2年前
  - 開発はそこそこ活発に行われている
- 0.6.0系と VNC バックエンドに別れを
  - 告げられるといいな

最近アクティブな開発者

- 開発チームの一員ではない
- Amazon.com の中の人
- C言語のエキスパート？
- warning を消したり
- const を付けたり
- とても助かっている

Pavel Roskin
proski

Amazon.com
Irvine, California, USA
Joined on 10 Jan 2012

新機能

- オーディオ転送がMP3をサポート
- SSL 3.0を無効化するオプションが追加
- TLS cipher suite を指定するオプションが追加

オーディオ転送の MP3 サポート

オーディオ転送の MP3 圧縮

- 9ccbfb6 で実装 (要LAME)
- サーバ/クライアント双方の対応が必要
  - Windows は対応している (7, 10)
- RDPのプロトコル上規定がない
  - 対応 codec を交換するフォーマットのみ規定
    - WaveInfo PDU [MS-RDPEA], WAVEFORMATEX
  - どの codec を実装すべきかは規定していない
  - クライアント依存 (PCMは基本的に対応)

xrdp のオーディオ転送

- 以下の codec に対応
  - PCM 44.1kHz 16bit 2ch (1411.2kbps)
  - PCM 22.05kHz 16bit 2ch (705.6kbps)
  - MP3 44.1kHz 16bit 2ch (128kbps)
  - Opus 48kHz 16bit 2ch

    (Opus は仕様で 48kHz のみ)
- クライアント・サーバ双方が対応しているものが使われる
- Opus対応クライアントってあるの？

Windows 7 から接続した場合

- RFC 2361
- PCM 44.1kHz 16bit
- PCM 22.05kHz 16bit
- MP3 44.1kHz 16bit
  - 128kbps
- C/S両方が対応のもの
- ブースでデモしてます

```
xrdp-chansrv [1727374209]: sound_process_output_format:
xrdp-chansrv [1727374209]:       wFormatTag      1
xrdp-chansrv [1727374209]:       nChannels       2
xrdp-chansrv [1727374209]:       nSamplesPerSec  44100
xrdp-chansrv [1727374209]:       nAvgBytesPerSec 176400
xrdp-chansrv [1727374209]:       nBlockAlign     4
xrdp-chansrv [1727374209]:       wBitsPerSample  16
xrdp-chansrv [1727374209]:       cbSize          0
xrdp-chansrv [1727374209]: sound_process_output_format:
xrdp-chansrv [1727374209]:       wFormatTag      1
xrdp-chansrv [1727374209]:       nChannels       2
xrdp-chansrv [1727374209]:       nSamplesPerSec  22050
xrdp-chansrv [1727374209]:       nAvgBytesPerSec 88200
xrdp-chansrv [1727374209]:       nBlockAlign     4
xrdp-chansrv [1727374209]:       wBitsPerSample  16
xrdp-chansrv [1727374209]:       cbSize          0
xrdp-chansrv [1727374209]: sound_process_output_format:
xrdp-chansrv [1727374209]:       wFormatTag      85
xrdp-chansrv [1727374209]:       nChannels       2
xrdp-chansrv [1727374209]:       nSamplesPerSec  44100
xrdp-chansrv [1727374209]:       nAvgBytesPerSec 176400
xrdp-chansrv [1727374209]:       nBlockAlign     4
xrdp-chansrv [1727374209]:       wBitsPerSample  0
xrdp-chansrv [1727374209]:       cbSize          12
```

SSL 3.0 の無効化

SSL 3.0 の無効化

- POODLE (CVE-2014-3356)
- パッチや設定では回避できないので
  使うのをやめるしかない
- 今や SSL 3.0 を使わないのは当たり前

という話は既によくご存知だと思います

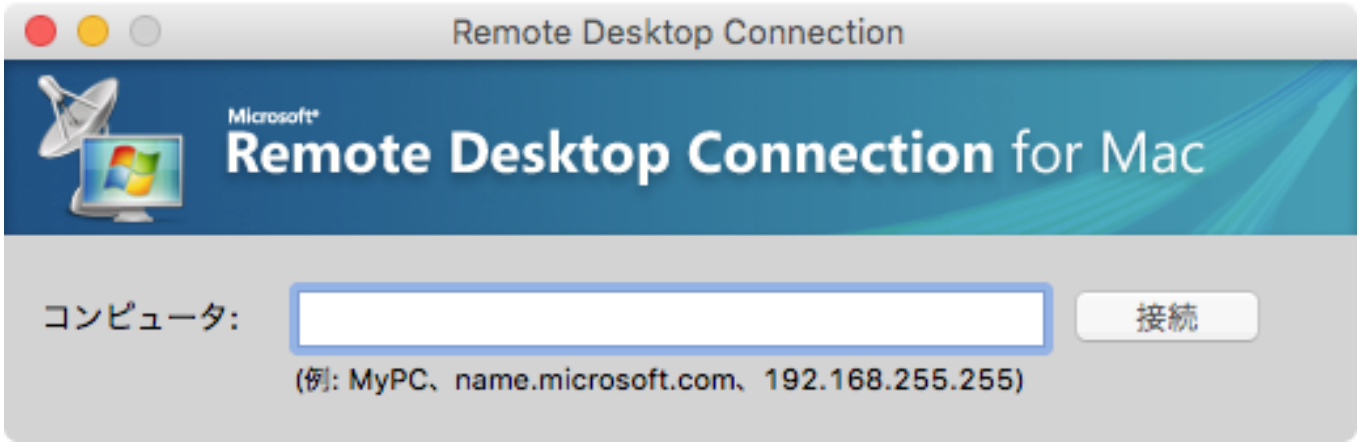
SSL 3.0 の無効化

- クライアントで対策が進んでいるので
  優先順位が低かった (e.g. Android)
- 通常は TLS 1.0 以降が使われる
  - SSL 3.0 に fallback する可能性があった
  - サーバ側でも SSL 3.0 を禁止できる方が安全
- 設定で SSL 3.0 を無効化出来るようになった

SSL 3.0 の無効化

- TLS非対応のクライアントでは接続できない
- オプションで無効化するかを制御できる
- SSL 3.0 のみ対応のクライアントは？
  - 調査した限りなかった
    - RDC for Mac
    - rdesktop
    - FreeRDP
    - Microsoft 製クライアント (含 iOS, Android)

SSL 3.0 の無効化



- SSL 3.0 を使うとソースコードにコメント
- しかし実際は TLS 1.0 にも対応している
- ただし暗号化は 3DES のみ対応

SSL 3.0 の無効化

- どうしても SSL 3.0 を使わざるを得ない場合
- xrdp.ini で設定する
  - disableSSLv3=yes|true|on|1 → SSL 3.0 無効
  - disableSSLv3=それ以外 → SSL 3.0 有効

```
14  # security layer can be 'tls', 'rdp' or 'negotiate'
15  # for client compatible layer
16  security_layer=rdp
17  # X.509 certificate and private key
18  # openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem -out cert.pem -days 365
19  certificate=
20  key_file=
21  # disable SSlv3
22  #disableSSLv3=yes
23  # set TLS cipher suites
24  #tls_ciphers=HIGH
```

xrdp の設定ファイル記法

- bool値の定義
- common/os_calls.c
- true, on, yes, 1 が ture として扱われる
- それ以外は false
- foo=enabled
  - foo=no と同じ

```
3325 /*****************************************
3326 /* returns boolean */
3327 int APP_CC
3328 g_text2bool(const char *s)
3329 {
3330     if ( (g_atoi(s) != 0) ||
3331          (0 == g_strcasecmp(s, "true")) ||
3332          (0 == g_strcasecmp(s, "on")) ||
3333          (0 == g_strcasecmp(s, "yes")))
3334     {
3335         return 1;
3336     }
3337     return 0;
3338 }
```

TLS cipher suite の指定

TLS cipher suite とは

ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS

TLS cipher suite とは

みたいなやつのことです

Apache や nginx の設定で見たことあるかも？

TLS cipher suite とは

- 暗号アルゴリズム (AES, Camellia, ...)
- 鍵長 (128bit, 256bit, ...)
- ハッシュ関数 (SHA-1, SHA-256, ...)
- 暗号利用モード (CBC, CFB, CTR, OFB, ...)

の組み合わせのこと

なぜ設定可能になったか

- SWEET32 (CVE-2016-2183)
  - 64 bit ブロックのTLS暗号に対する誕生日攻撃
  - DES/3DES や Blowfish が該当する
- OpenSSL はこのように対応
  - 3DES を HIGH から MEDIUM に降格
  - 深刻度は moderate (全4分類中上から3番目)
- xrdp でも設定できたほうが脆弱性対策できる

SWEET32 脆弱性への対応

- xrdp の設定で回避する場合
  - xrdp.ini を書き換え: tls_ciphers=HIGH:-3DES
  - HIGH から 3DES 除いた暗号方式を使う
  - OpenSSL とやっていることは同じ

TLS cipher suite の指定

- コメントアウトは外しておきましょう
  - 最低でも HIGH にしておいたほうが良い
- クライアントの兼ね合いもある
  - 古いクライアントを受け入れる場合
  - 旧式の暗号アルゴリズムの使用は自己責任で
- どのクライアントがどれに対応している？
  - オープンソースじゃないからわからない

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

Android 版 Microsoft 公式クライアントで
接続できない問題

これ→

Android 版 MS 公式クライアント

- neutrinolabs/xrdp#246
- 接続しようとすると0xd06エラーになる
- iOS 版では起きない
- クライアント側の問題？
  - そうもいってられない
  - MS製品同士での接続には何の問題もない
  - xrdp 側で対処することにした
- もう少し待っていてください

Android 版 MS 公式クライアント

- 実は Windows 版もある
- msctsc.exe じゃない方
- Windows ストア版
  - まだまだ開発途上
  - コードベースは Android 版と同じ？
- xrdp との接続性に問題あり
- プロトコルのドキュメントと異なる動きをする

xrdpの導入や開発

xrdpの導入や開発

- OSS とはいえビジネス的要素は避けられない
- スポンサー付きのバグほど修正は早い
  - 最近修正されたバグにもスポンサーが
  - Android 版クライアントの問題もおそらくそう
- 日常の使用に支障のあるバグは少なくなった
  - まだまだ改善の余地がある

xrdpの導入や開発

- なぜその機能が必要なのか具体的な背景があると優先度が上がりやすい

  例:

  PCI-DSS v3.1に準拠するため TLS v1.0 を無効化できる機能が必要 など

xrdpの導入や開発

- この機能のバグが修正されたら導入する
- この機能が実装されたら導入できる
- 等々の事情がある方
  - 後で個人的にご相談ください

ここから質問に答えていきます

ハッシュタグ #xrdp_jp をつけてツイート
次回 Tokyo/Spring のセミナーの参考にします