

KDDI Flex Remote Access

**VPN 接続手順・**  
**VPN クライアントソフト操作マニュアル**

Android™ OS 版<sub>(4.0 以降)</sub>

2018 年 7 月  
KDDI 株式会社

Ver1.9

1	はじめに.....	3
2	Android™ OS での KDDI Flex Remote Access のご利用.....	4
2.1	Android™ OS 接続について.....	4
2.2	接続環境について.....	4
2.3	接続設定について.....	4
3	端末設定方法.....	5
3.1	インストール権限.....	5
3.2	Google Play ストアへのアクセス.....	5
3.3	ソフトウェアのインストール.....	6
3.4	VPN に関する設定.....	7
3.5	接続方法.....	10
3.6	接続解除の方法.....	13
3.7	設定項目を誤入力した場合.....	14
4	証明書を利用した認証をご契約の場合.....	15
4.1	証明書の選択.....	15
4.2	オンデマンド接続機能.....	15
5	各種情報の表示 / トラブルシューティング.....	16
5.1	各種統計情報.....	16
5.2	トラブルシューティング.....	17

## 1 はじめに

- ※ 本資料に記載されている内容に関しましては、KDDI 株式会社の都合により変更することがある旨をご了承ください。
- ※ 本サービスご利用前に、本資料を必ずお読みください。
- ※ 免責事項・注意事項をご承諾いただけない場合、本サービス利用はお控えください。

本資料の一部または全部を「KDDI Flex Remote Access」の利用者もしくは運用者以外に対して開示・配布・譲渡すること、「KDDI Flex Remote Access」以外の利用目的にて用いることを禁じます。

本資料は、「KDDI Flex Remote Access」をご利用いただく上で最低限の事項のみ記述しています。KDDI は本資料の作成に当たり、サービス提供上問題が発生しないよう、細心の注意を払っていますが、この資料に記載された内容に準拠した端末設定にて利用された場合においても、KDDI はお客さまアプリケーションの接続性を保証するものではありません。

「KDDI Flex Remote Access」上でご利用になられるアプリケーションに関する一切の質問は、受け付けることができません。アプリケーションおよびサーバ・ルータなどネットワーク機器に関するお問い合わせは導入ベンダー/メーカーさまへお問い合わせください。

設定方法・仕様などは、KDDI の都合により、予告なしに変更される可能性がありますのであらかじめご了承ください。なお、問題点・変更点などを発見した場合は、お手数ですが KDDI 法人営業担当者までお気付きの点をご連絡ください。今後の資料作成に反映させていただきます。

## 2 Android™ OS での KDDI Flex Remote Access のご利用

### 2.1 Android™ OS 接続について

「KDDI Flex Remote Access」は、パソコン・スマートフォン・タブレット端末から、専用閉域網・インターネットを経由して「KDDI Wide Area Virtual Switch」への接続を可能とするリモートアクセス型サービスです。「KDDI Flex Remote Access」は、パソコン・スマートフォン・タブレット端末に専用の VPN ソフトウェアをインストールし接続を実現します。

Android ™端末には、Google Play ストアより専用の VPN ソフトウェアをダウンロード / インストールしていただくことで「KDDI Flex Remote Access」をご利用いただけます。

### 2.2 接続環境について

「KDDI Flex Remote Access」は、SSL-VPN 機能を拡張した VPN 技術を利用しています。お客さまご利用環境下において、UDP:53(DNS) / TCP:443(TLS) / UDP:443(DTLS)の疎通が確保できている必要があります。

また Proxy サーバ経由での接続も可能ですが、Proxy サーバにおいて TCP:443(TLS) / UDP:443(DTLS)の接続が確保されている必要があります。

※Proxy サーバ経由での接続の場合、VPN 内通信に対しての通信時も Proxy 設定を流用してしまうため、Proxy 経由通信については注意が必要です。

※DTLS 通信(UDP:443)が利用できる環境下においてファイアウォールが介在する場合は、ファイアウォールセッション消失の可能性があるため、UDP セッション維持時間を長めにする必要があります。(UDP セッション維持時間の設定が短いと、通信途中で VPN が不安定になる(応答がなくなる)事象が発生する可能性があります)

### 2.3 接続設定について

Android ™ 4.2 以上の au 端末をご利用の場合、Android ™ の設定で『Wi-Fi 安定制御機能』を『OFF』にすることを推奨します。

※「KDDI Flex Remote Access」の接続先登録を『デフォルト(すべての通信)』としてご利用されているお客さまが、本機能を ON のまま VPN 接続を行うと、通信途中で VPN が不安定になる(切断・再接続を繰り返す)事象が発生する可能性があります。

※ 端末側の設定は、『設定』→『Wi-Fi』→『詳細設定』→『Wi-Fi 安定制御機能』と操作してチェックを外します。(設定箇所は、端末によって異なる場合があります。詳しくは端末のマニュアルなどをご確認ください)

### 3 端末設定方法

以下の手順にてスマートフォンを設定いただきます。なお、証明書認証をご利用の場合、証明書のインストールと合わせて AnyConnect をインストールしますので、既に証明書および AnyConnect をインストール済のお客さまは『3.4 VPN に関する設定』から実施してください。

#### 3.1 インストール権限

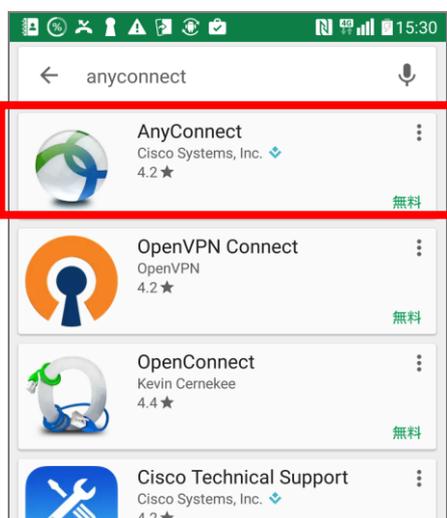
クライアントソフトウェアをインストールするための権限を保有していることが必要です。

#### 3.2 Google Play ストアへのアクセス



Google Play ストアへアクセスします。  
※ご利用には Google アカウントが必要です。

入力欄に『AnyConnect』と入力し、検索を実行します。

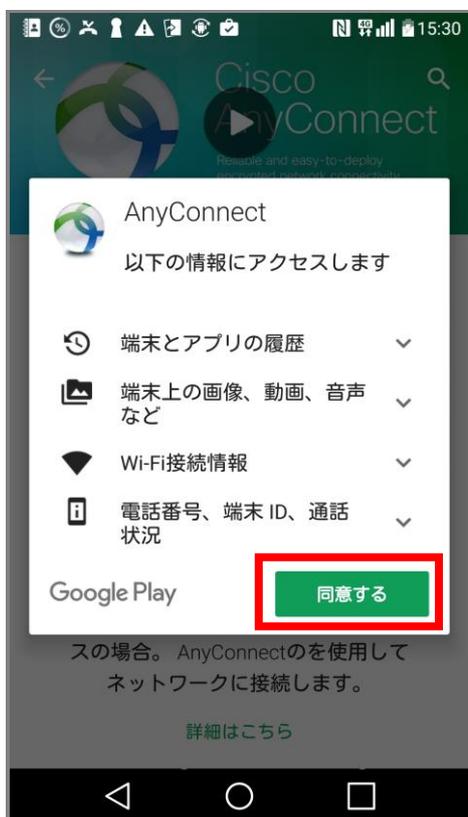


検索により表示された  
『AnyConnect』を選択します。  
※バージョンは画面と異なる場合があります。

### 3.3 ソフトウェアのインストール



『インストール』を選択します。



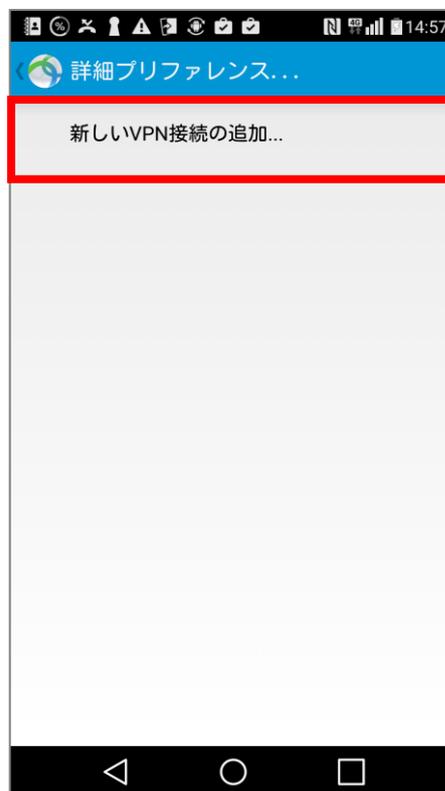
『同意する』を選択すると、インストールが開始されます。

### 3.4 VPNに関する設定



インストールの完了後、『開く』を選択し、ソフトウェアを起動し設定を開始します。  
※初期設定完了後は、ショートカットなどから起動します。

VPN 接続に関する設定を投入するため『新しい VPN 接続の追加』を選択します。





接続に必要な項目を入力します。

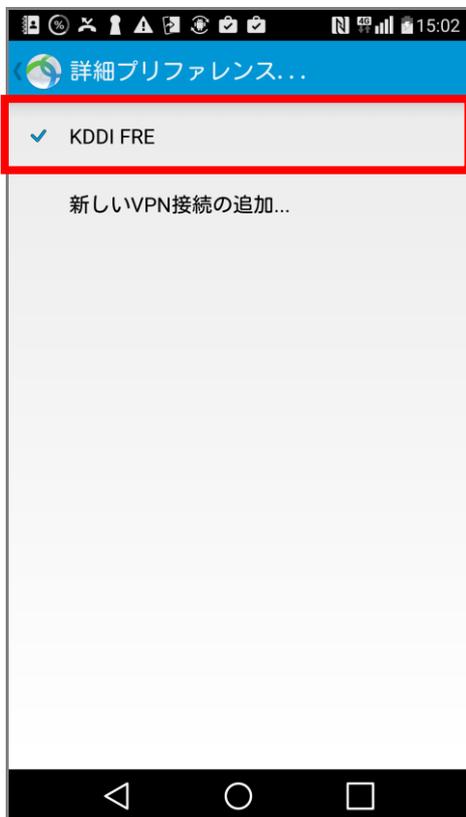
項目	入力内容
説明	任意の名称を入力
サーバ	開通案内記載の接続先 URL(https://gwXX...)を入力 ●証明書認証を利用しない場合 『Host 名/XXX_XXXX』形式(https://gwXX...jp/XXX_XXXX)での入力 ●証明書認証を利用する場合 Host 名までを入力(https://gwXX...jp)
証明書	自動(後述 4 項にてご説明します。)



入力が完了したら、左図のような設定となります。  
(※実際はサーバの URL 値も表示されます)

入力が完了したら、『完了』ボタンをタップしてください。

VPN 設定画面に戻ると作成したエントリが表示されます。



### 3.5 接続方法



AnyConnect のトップ画面から、該当のエントリに対して、『AnyConnect VPN』を『オン』にします。

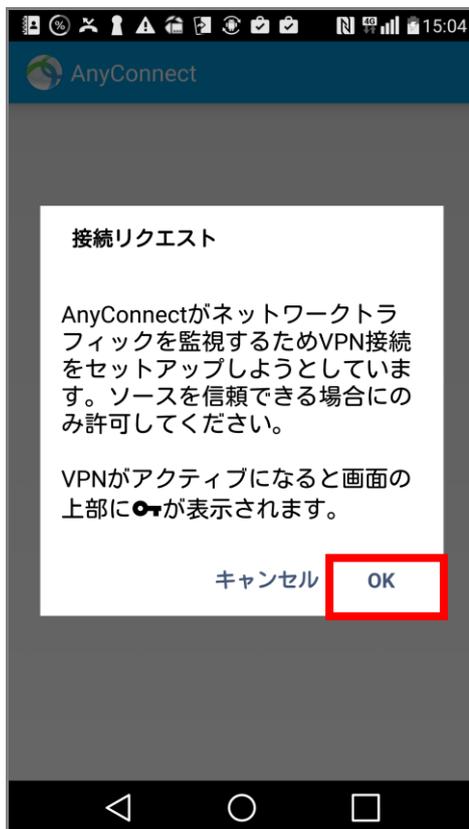
※ Close 網をご利用の際は、本接続の前に Close 網の接続を行ってください。Close 網の接続方法(ID など)は、KDDI 法人営業担当者へご確認ください。



お客さまご利用環境により左図のような確認表示がされる場合があります。その場合は『承認』を選択してください。



お客さま管理者さまより指定された、『ユーザ名』と『パスワード』を入力してください。ユーザ名は、@を含むメールアドレス形式でご入力ください。(xxxxx@suffix 名) 入力後『接続』を選択してください。



左図の画面が表示された場合は、『OK』を選択します。



接続が完了すると、左図のように『オン』となり、『接続済み』と表示されます。

### 3.6 接続解除の方法



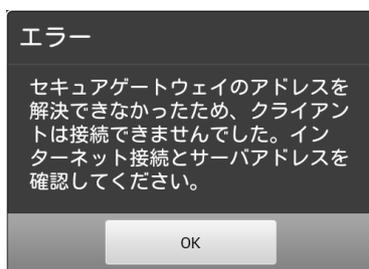
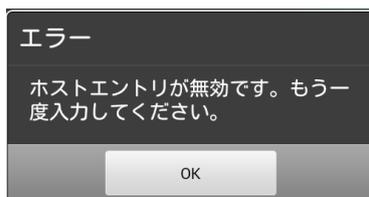
『AnyConnect VPN』を『オフ』に変更します

### 3.7 設定項目を誤入力した場合

各設定項目の入力を間違った場合、各種エラー表示が出ます。

#### ■ エラー表示の例

- ユーザー名 / パスワード入力が間違っていた場合、再度ログイン ID とパスワードを求められます。
- 接続用 URL 設定が間違っていた場合



※入力された結果によりエラー表示は異なります。

通常とは異なる表示が出た場合は、各種設定を再度ご確認ください。

## 4 証明書を利用した認証をご契約の場合

### 4.1 証明書の選択

証明書を利用した認証オプションをご契約の場合は、事前にサイバートラスト社より通知されるメールに基づき証明書をインストールしていただく必要があります。

※証明書のインストール方法は、別途『[証明書インストールマニュアル Android™OS 版](#)』を参照ください。

複数枚の証明書が既にインストールされている場合は、以下手順で接続に利用される証明書を選択することをおすすめします。



『詳細プリファレンス』から『証明書』をタップします。

※ご利用のバージョンによっては、表記が異なる場合があります。



接続に利用する証明書を選択し、チェックを入れます。

### 4.2 オンデマンド接続機能

Android (TM) OS ではサポートされていません。

## 5 各種情報の表示 / トラブルシューティング

接続時の情報を表示することが可能です。

### 5.1 各種統計情報



AnyConnect のトップ画面から『詳細…』を選択します。

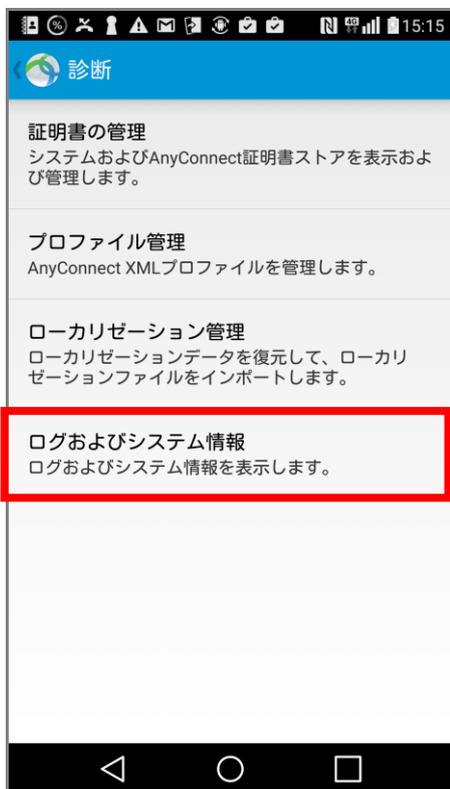


詳細な統計情報が表示されます。

## 5.2 トラブルシューティング



メニューボタンから『診断』を選択します。  
※端末によりメニューボタンの位置は異なります。

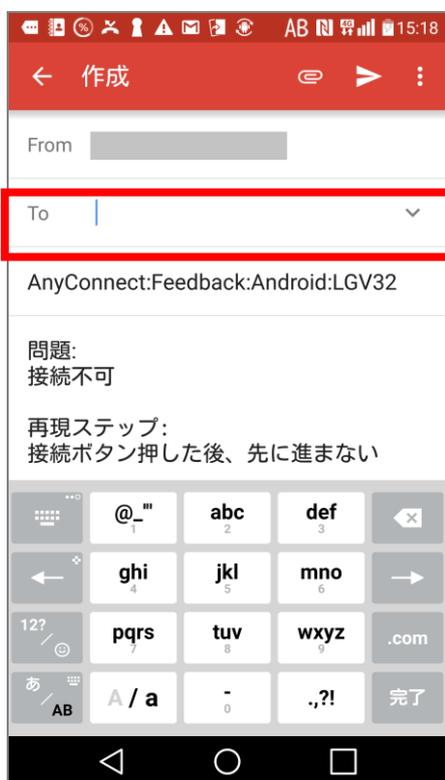


『ログおよびシステム情報』を選択します。



メニューより『ログの送信』を選択し、問題点および手順概要を入力します。

その後『管理者にレポート』を選択します。



メールアプリケーションを選択した場合、メールクライアントが立ち上がり、デバッグログを纏めたファイルができあがります。

KDDI サービスコントロールセンター(SCC)指定のアドレスか、お客さま管理者さまへご送付ください。

※宛先、件名については KDDI TSC もしくはお客さま管理者さまの指示に従ってください。

以上

## 改版履歴

- ◆ 2012年 5月 21日 Ver 1.0 リリース
- ◆ 2012年 12月 17日 Ver 1.1 証明書認証対応
- ◆ 2013年 2月 7日 Ver 1.2 証明書選択手順の変更
- ◆ 2013年 3月 19日 Ver 1.3 接続環境の注意事項追記
- ◆ 2013年 8月 6日 Ver 1.4 クライアントソフトウェアの画像更新
- ◆ 2013年 8月 23日 Ver 1.5 接続先 URL の表記を修正、Close 網の場合の注意事項を追記
- ◆ 2013年 10月 30日 Ver 1.6 Android4.2 の場合の Wi-Fi の設定の注意事項を追記
- ◆ 2014年 4月 7日 Ver 1.7 ドキュメントタイトル修正
- ◆ 2017年 3月 24日 Ver 1.8 AnyConnect 画面など更新
- ◆ 2018年 7月 1日 Ver 1.9 KDDI サービスコントロールセンターへ改称に伴う修正