KDDI Flex Remote Access

KDDI ビジネスセキュアWi-Fi

証明書インストールマニュアル

Windows(R) 10 Mobile 版

Ver.1.0

2016 年 11 月

KDDI 株式会社

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。

※「KDDI Flex Remote Access」および「KDDI ビジネスセキュア Wi-Fi」の両サービス（以下『両サービス』）において証明書認証機能（以下『本機能』）のご利用前に、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、本機能のご利用はお控えください。

本資料の一部または全部を両サービス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、両サービス以外の利用目的にて用いることを禁じます。

本資料は、両サービスにおいて本機能を利用する際に必要となる証明書をご利用端末にインストールする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手順にて利用された場合においても、端末の機種や OS のバージョンにより証明書をインストールできない可能性があります。その場合は KDDI 法人営業担当まで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 法人営業担当まで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。

※両サービスでは、証明書の発行をサイバートラスト株式会社へ委託しており、サイバートラスト株式会社の『サイバートラスト　デバイス ID』を使用します。

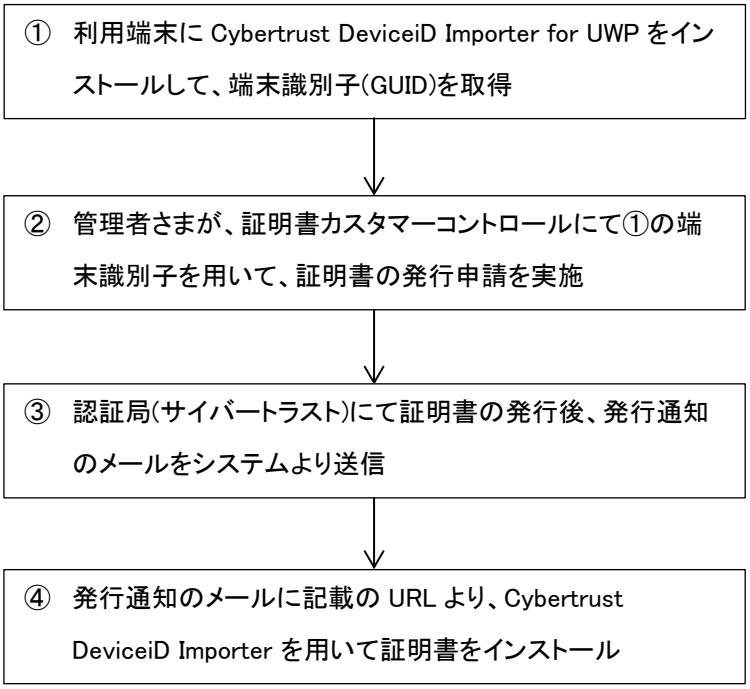
※両サービスでは、それぞれのサービスで提供する証明書以外はご利用できません。既にサイバートラスト社の証明書をご利用されている場合でも両サービスで提供する証明書以外のご利用はできません。

※本資料内の画面および証明書ダウンロード用 URL は実際とは異なる場合がありますので、あらかじめご了承ください。

1. 概要

1.1. Windows(R) 10 mobile 端末への証明書インストール手順概要

お客さま管理者さまにより発行された証明書を Windows(R) 10 mobile 端末へ個別に取得、インストールすることができます。インストールまでの手順の概要は以下の通りです。



※ 証明書の発行通知メールの送信者メールアドレス(Fromアドレス)が、<no-reply@deviceid.kddi.ne.jp>の場合、このメールアドレスはシステムの自動送信用のアドレスのため、このメールアドレスへ返信されても対応はできませんのであらかじめご了承ください。対応が必要な場合は、貴社システム管理者さまへご連絡をお願いします。

※ セキュリティ上、証明書がインストール可能な期間が設けられています。発行通知メール受信後、下記取得期限内に証明書のインストールを完了させてください。

- 証明書発効日(メール送信日)から7日間、または証明書の初回ダウンロードから3日間

取得期限を超えた場合は、証明書を取得できなくなります。その場合は、お客さま管理者にて『取得可否変更』の操作を行うことで再度取得可能になります(変更後も同様の取得期限があります)。

※ 管理者が証明書発行時に指定したWindows(R) 10 Mobile端末以外には証明書をインストールできません。

2. 証明書発行前の事前準備

ここでは、Windows(R) 10 Mobile 端末向けに証明書を発行するための事前準備について説明します。

管理者が Windows(R) 10 Mobile 端末向けに証明書を発行するためには、事前に端末識別子(GUID)を取得し、管理者へ伝える必要があります。GUID の取得・通知は Cybertrust のアプリケーションを利用します（Cybertrust DeviceiD Importer for UWP）。

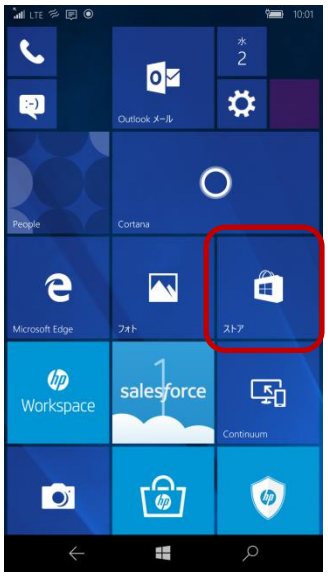
2.1. Cybertrust DeviceiD Importer for UWP のインストール

証明書をインストールする端末に Cybertrust DeviceiD Importer for UWP をインストールします。Windows(R)ストアからアプリケーションをダウンロードする際には Microsoft(R)アカウントが必要になります。

(1) Windows(R) ストアにアクセスします。

(2) 『Cybertrust DeviceiD Importer』を検索します。

(3) 『Cybertrust DeviceiD Importer』 をインストールします。



2.2. 端末識別子(GUID)の取得と通知

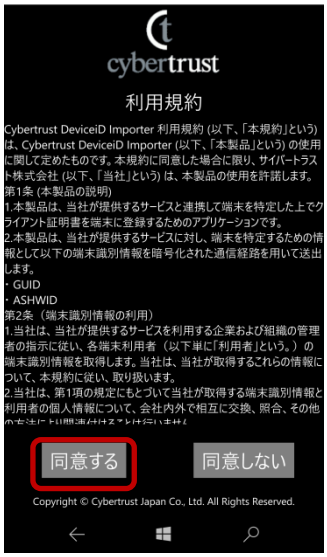
証明書をインストールする端末の端末識別子(GUID)を取得して、管理者へ提出します。

【すべてのアプリ】から【Cybertrust DeviceiD Importer】を選択し、起動します。

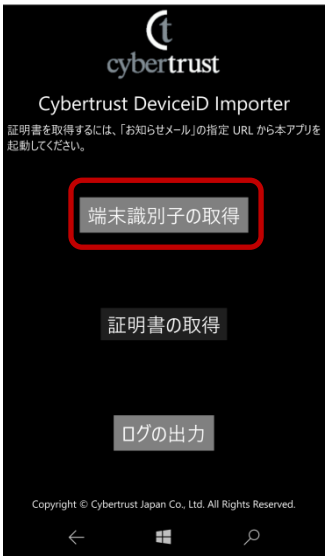
初回起動時には右図のように利用規約が表示されます。

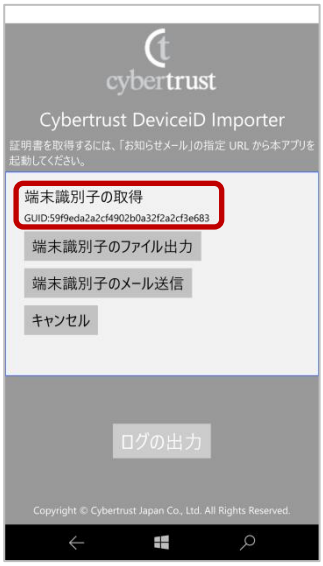
内容をご確認の上、【同意する】をタップします。

※ 一度【同意する】をタップすると、次回以降の起動時には利用規約は表示されません。



(1) 【端末識別子の取得】をタップすると、端末識別子が表示されます。





(2) 端末識別子の出力方法を選択します。管理者の指示がある場合は、その方法に従ってください。

- 【端末識別子のファイル出力】

  『ファイル名』と『ファイルの保存場所』を指定して、端末識別子ファイルを保存できます。

- 【端末識別子のメール送信】

  デフォルトに設定しているメールソフトが起動し、本文に端末識別子が記載されたメールが新規に作成されます。

※【キャンセル】をタップするとメニュー画面に戻ります。

【ご注意】

証明書をインストールする際に端末識別子が合致していないと、証明書はインストールされません。端末識別子(GUID)は、本アプリケーションが作成しているため、端末識別子取得後に本アプリケーションを削除・アンインストールをしないようお願いします。

※ 本アプリケーションを再インストールした場合、端末識別子が変わります。

もし証明書のインストールの前に本アプリケーションを削除・再インストールした場合は、改めて端末識別子を取得し、管理者にて証明書を新たに発行していただければ証明書のインストールは可能です。

---

3. 証明書のインストール

『2. 証明書発行前の事前準備』にて取得した端末識別子を用いて、管理者が証明書を発行します。証明書発行後、発行通知メールを受信したら本作業を行います。

(1) ユーザに証明書発行通知メールが届きます。

(2) メールに記載されている手順の通り、URL をタップして証明書をインストールします。インストールの際は Cybertrust DeviceiD Importer を用います。

【ご注意】

セキュリティ確保の目的から、証明書の取得期限がありますので、メールを受信したら期限内に証明書をインストールしてください。

- 取得期限: 証明書発行(メール送信日)から7日間、または証明書の初回ダウンロードから3日間

取得期限を超えた場合は、証明書を取得できなくなります。その場合はお客さま管理者にて該当証明書の『取得可否変更』を行うことで、再度取得可能になります(変更後も同様の取得期限がございます)。

3.1. Windows(R) 10 Mobile への証明書インストール

(1) インストールする Windows(R) 10 mobile 端末にて、証明書発行通知のメールを確認します。メールの本文内の手順 1 に『認証コード』が記載されている場合は、『認証コード』を選択してあらかじめコピーしておきます。(『認証コード』が記載ない場合は不要です)

件名: **サイバートラスト デバイス ID 発行のお知らせ**
KDDI 株式会社の申請により、デバイス ID が発行されました。 利用約款および認証局運用規程(CPS)をご確認のうえ、デバイス ID をインストールしてください。 デバイス ID は発行から 7 日を経過するとインストールできなくなります。 お早めのインストールをお願いいたします。 発行から 7 日を経過した場合は、管理者へお問い合わせください。 利用約款および認証局運用規程(CPS)は以下から参照してください。 https://www.cybertrust.ne.jp/deviceid/repository.html 手順 1: 以下の URL をタップして「Cybertrust DeviceiD Importer」を起動してください。 cybertrust://?sd=DiDk&cd=G3k&pd=DeviceiD_KDDI_UCS_GUID_UWP&rd=201610140151255&rfd=1E43VGtl

「認証コード」の入力を求められた場合は、以下の「認証コード」を入力して「送信」をタップすると、
デバイス ID がインストールされます。
　認証コード: **********

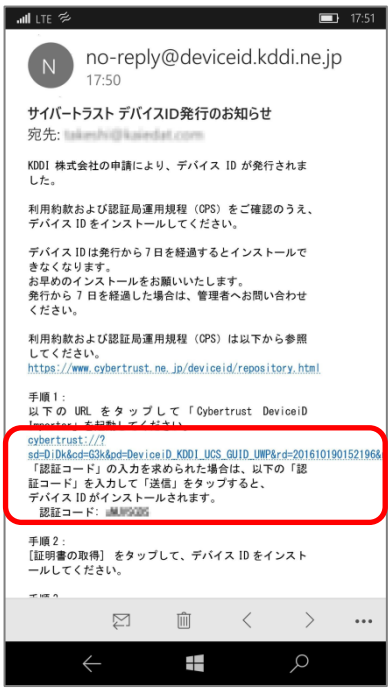
手順 2:
[証明書の取得] をタップして、デバイス ID をインストールしてください。

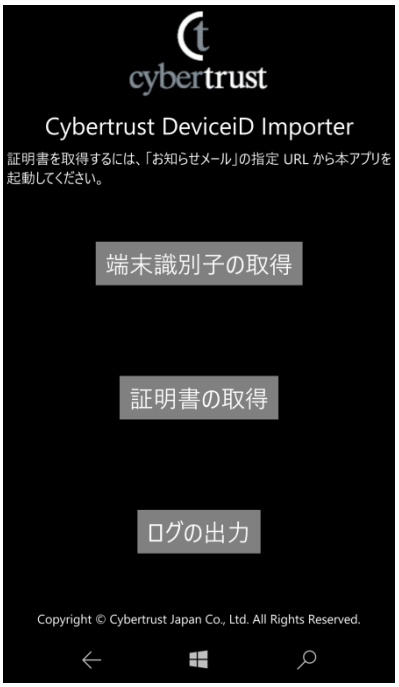
デバイス ID 情報
　リクエスト ID　: 20**********
　コモンネーム　: xxxxx@suffixname
　シリアル番号　: ********
　証明書有効期間: 2016/**/**-**:**:** - 2021/**/**-**:**:**

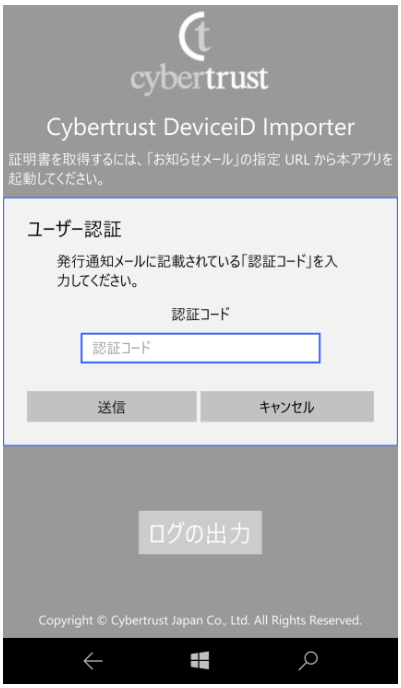
デバイス ID のインストールについてご不明な点がありましたら、
貴社システム管理者さまへお問い合わせください。

KDDI 株式会社
証明書発行担当
---

(2)　証明書発行通知メールに記載された手順1について、『認証コード』が記載されている場合はあらかじめその値をコピーします。記載されていない場合は、そのまま URL をタップします。







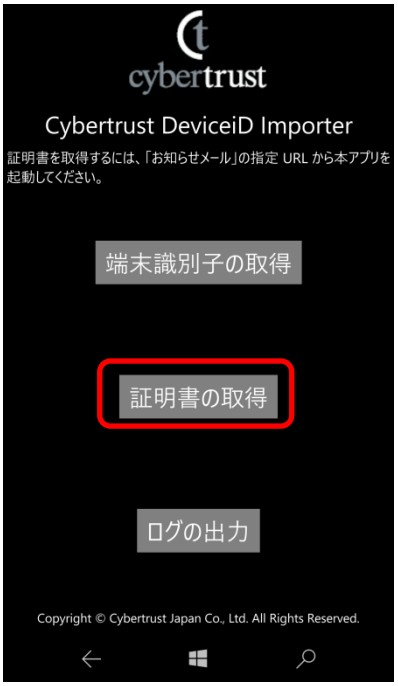
メールの手順 1 記載の指定 URL より、Cybertrust DeviceiD Importer を起動します。

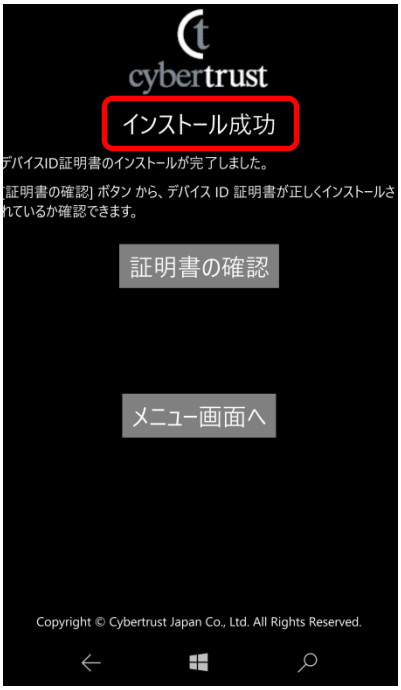
上の画面が表示された場合は、メールの手順 1 に記載されている『認証コード』を入力し【送信】します

【ご注意】

ブラウザなどでメールを開いた場合、手順1のリンクが有効にならない場合がございます。
Outlook(R)アプリケーションでメールを開くことをおすすめします。

(3) 【証明書の取得】をタップして、証明書をインストールします。完了するまでしばらくお待ちください。インストールが完了すると『インストール成功』の画面が表示されたらインストールは完了です。

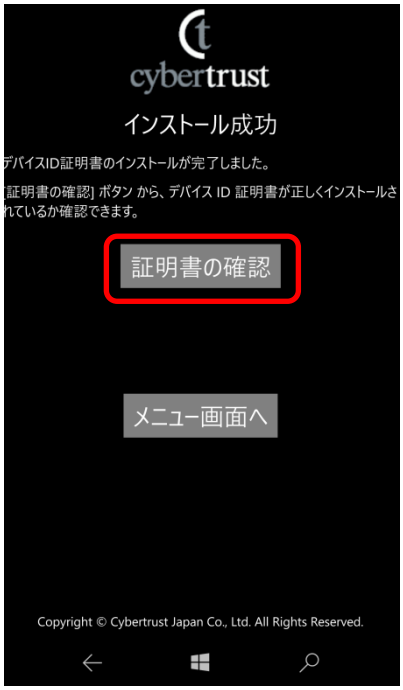




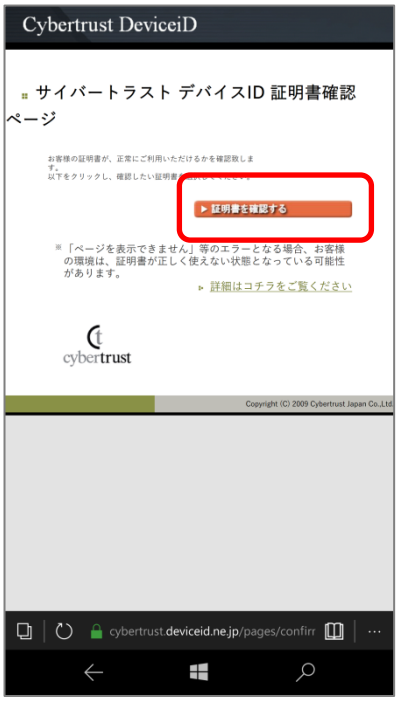
3.2. インストールした証明書の確認

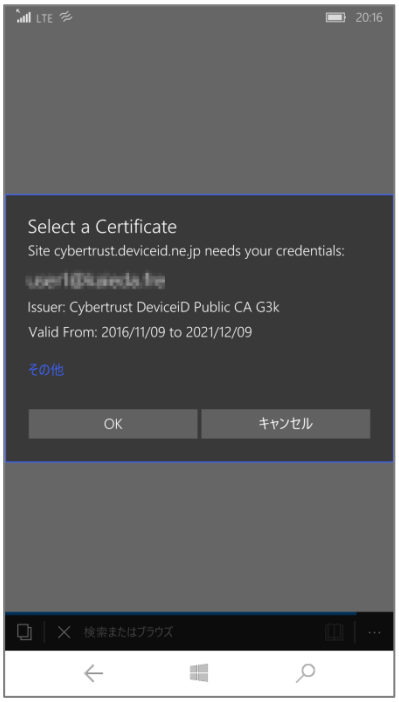
(1) インストールした証明書を確認するには、【証明書の確認】をタップするか、次の URL にアクセスすることでサイバートラスト社の確認ページへアクセスできます。

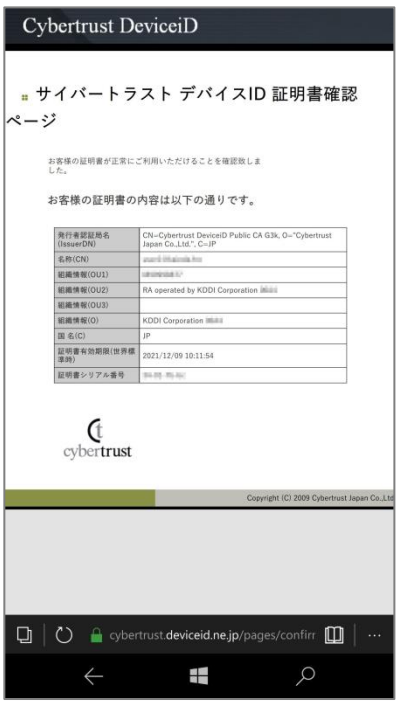
- https://cybertrust.deviceid.ne.jp/confirm.info/



(2) サイバートラスト社の証明書確認ページ（サイバートラスト社ウェブサイト）にアクセス後、【証明書を確認する】ボタンをタップします。証明書の選択画面(Confirm Certificate)が表示された場合は、該当の証明書を選択します。証明書情報が表示されれば問題ありません。







3.3. トラブルシューティング

3.3.1. エラーメッセージと主な対処方法

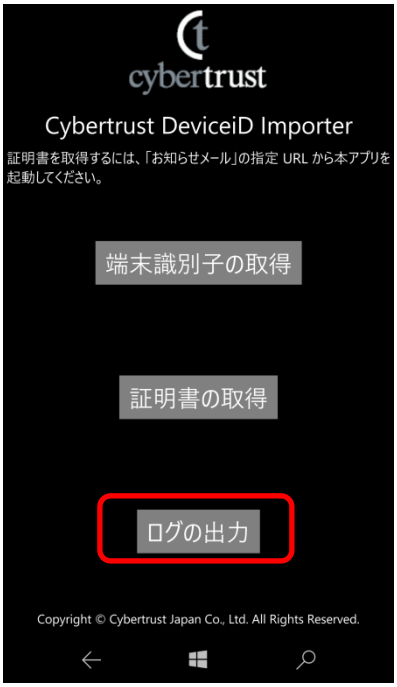
ここでは、エラーが発生して証明書のインストールができない場合について説明します。Cybertrust DeviceiD Importer をご利用中にエラーメッセージが表示された場合は、下記の表をご参考にしてください。

エラーメッセージ	対処方法
400 端末の認証に失敗しました。リクエスト ID と端末識別子を管理者に知らせてください。	端末識別子（GUID）が合致していない可能性があります。エラーメッセージの内容と『お知らせメール』に記載されている『リクエスト ID』、および Cybertrust DeviceiD Importer で参照できる『端末識別子』を控え、お客さま管理者にお問い合わせください。 端末識別子が合致していない場合は、管理者にて証明書の発行を再度行ってください。端末の利用者は証明書のインストールが完了するまで Cybertrust DeviceiD Importer を削除しないでください。
402 ユーザ認証に失敗しました。入力内容を確認してください。改善しない場合は管理者にお問い合わせください。	認証コードに問題がある可能性があります。『お知らせメール』に記載されている認証コードをご確認ください。 認証コードが正しい場合は、エラーメッセージの内容と『お知らせメール』に記載されている『リクエスト ID』を控え、お客さま管理者にお問い合わせください。
501 ただ今、サービスがメンテナンス中のためご利用頂けません。明日、改めて実施してください。	認証局（サイバートラスト社）設備がメンテナンス中です。メンテナンス終了後、改めて実施してください。
502 通信が切断されました。通信状況の良い場所で改めて実施してください。改善しない場合は管理者にお問い合わせください。	通信障害などの原因によりエラーが発生しました。時間を空けて、改めて実施してください。
600 証明書の登録に失敗しました。アプリを再起動して改めて実施してください。改善しない場合は管理者にお問い合わせください。	Cybertrust DeviceiD Importer の起動中に何らかのエラーが発生しました。アプリケーションまたは端末を再起動して改めて実施してください。改善しない場合はお客さま管理者経由で KDDI 法人営業担当へお知らせください。
601 端末識別子の取得に失敗しました。アプリを再起動して改めて実施してください。改善しない場合は管理者にお問い合わせください。	端末識別子のデータが破損している可能性があります。新規に証明書の発行申請が必要です。お客さま管理者にお問い合わせください。
603 不明なエラーが発生しました。管理者にお問い合わせください。	アプリケーションのバージョンが古い可能性があります。アプリケーションをアップデートして改めて実施してください。改善しない場合は、お客さま管理者経由で KDDI 法人営業担当へお知らせください。

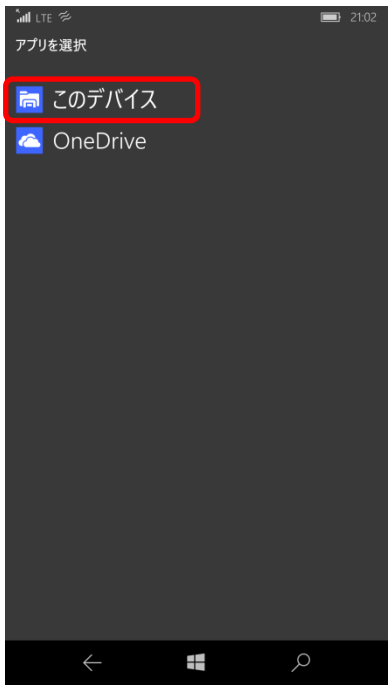
3.3.2. アプリケーションログの取得方法

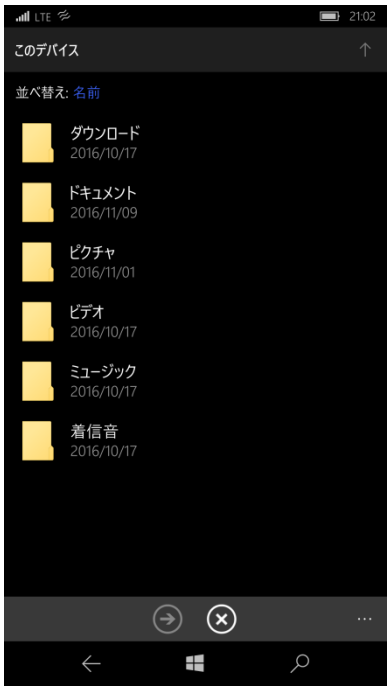
『3.3.1 エラーメッセージと対処方法』に記載の方法で改善しない場合、ログを取得して調査することが可能です。

（1） Cybertrust DeviceiD Importer の画面より【ログの出力】をタップします。



（2） 保存場所は【このデバイス】とし、任意のフォルダーを指定してください。【保存】ボタンをタップすると、テキストファイルで保存されます。保存したログファイルは、KDDI 法人営業担当へお送りください。





改版履歴

◆2016 年 11 月 16 日　　v1.0 リリース