KDDI Flex Remote Access

KDDI ビジネスセキュア Wi-Fi

証明書カスタマーコントロール
操作マニュアル

第 4.0 版

2019 年 12 月

KDDI 株式会社

目次

はじめに 5

1 証明書カスタマーコントロールについて 6

1.1 概要 6

1.2 ご利用環境 6

1.3 アクセス先 URL 8

1.4 本システムでの用語の説明 9

2 証明書の管理・運用方法 11

2.1 証明書管理の概要 11

2.2 証明書のステータスについて 12

2.3 発行/失効申請処理時間 14

2.4 機能一覧 15

3 ログイン操作 17

3.1 初回ログイン 17

3.2 2 回目以降のログイン 17

3.3 パスワードロック 18

3.4 トップ画面 18

3.5 ログアウト操作 19

4 証明書の発行申請 20

4.1 「KDDI FRE」で iOS/iPadOS デバイスをご利用のお客さま 20

4.2 証明書の発行申請メニュー 21

4.3 証明書の発行申請 21

4.4 証明書の一括発行申請 27

5 証明書の失効申請 32

5.1 証明書の失効申請 32

5.2 証明書の一括失効申請 35
5.3 申請エラーについて 36
6 証明書の管理 37
6.1 申請情報の検索 37
6.2 証明書の取得可否変更 46
6.3 証明書のステータス更新 50
6.4 通知用アドレス一括変更 51
7 構成プロファイルの管理 52
7.1 構成プロファイルの作成方法 53
7.2 構成プロファイルの登録 55
7.3 構成プロファイルの配布 55
7.4 構成プロファイルの変更 56
7.5 構成プロファイルの削除 57
7.6 証明書カスタマーコントロールのメニュー 58
7.7 構成プロファイルの登録・削除 59
7.8 構成プロファイルの簡易作成 63
7.9 構成プロファイルの変更 65
8 レポートの出力 66
8.1 証明書のレポート 66
8.2 証明書のサマリレポート 70
9 監査 71
9.1 ログの検索 71
10 管理者アカウント 72
10.1 パスワードの変更 72
10.2 有効期間終了通知設定 73
11 オンライン・ヘルプ 74
11.1 マニュアル 74

11.2 お知らせ 74
12 各種処理状況の確認 75
12.1 各処理のステータス 75
12.2 証明書の詳細ステータス 76
13 各種フォーマット(メールフォーマット/各種申請 CSV フォーマット) 79
13.1 メールフォーマット 79
13.2 各種申請 CSV フォーマット 87
14 お問い合わせ窓口 93
15 定期メンテナンス 95

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で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 法人営業担当者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。

※ 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になれません。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。

1　証明書カスタマーコントロールについて

1.1　概要

証明書カスタマーコントロールは、お客さまの管理者さま(以下、管理者さま)による端末認証のための証明書を発行または失効などを行うシステムです。この証明書は「KDDI FRE」または、「KDDI ビジネスセキュア Wi-Fi」の証明書認証(端末認証)にご利用いただけます。

構成について、お客さま側にカスタマーコントロール用の端末（以下『カスタマーコントロール端末』）より、ウェブベースで KDDI の証明書カスタマーコントロールサーバーにアクセスしていただきます。カスタマーコントロール端末～証明書カスタマーコントロールサーバーへはインターネット経由(SSL)で接続します。

お客さまがカスタマーコントロールサーバー経由で申請処理された内容は、認証局へ送信され発行/失効処理が実施されます。

1.2　ご利用環境

(1) 推奨パソコン ： Windows® 7・10

(2) 推奨ブラウザ ： Microsoft Internet Explorer® 11（日本語版）

※ すべての端末でのご利用を保証するものではありませんので、事前に試験環境などでご確認ください。

※ Firefox®など Internet Explorer®以外のブラウザをご利用の場合、レイアウトのずれ、または文字化けなどが発生する場合があります。

(3) ブラウザの設定

本システムでは、JavaScript・Cookie・TLS を有効にする必要があります。設定方法は以下のとおりです。

項目	Internet Explorer®の設定
1)JavaScript を有効にする	以下の項目を有効にします。 **→【ツール】→【インターネットオプション】** **→【セキュリティ】** **→【レベルのカスタマイズ】** **スクリプト** ・【アクティブスクリプト】 **ダウンロード** ・【ファイルのダウンロード】
2)Cookie を有効にする	以下の項目を有効にします。 **→【ツール】→【インターネットオプション】** **→【プライバシー】→【詳細設定】** ・①【自動 Cookie 処理を上書きする】をチェック（IE 9） ・②【ファーストパーティの Cookie】ー承諾する ・③【サードパーティの Cookie】ー承諾する
3)TLS を有効にする	以下の項目を有効にします。 **→【ツール】→【インターネットオプション】** **→【詳細設定】→【セキュリティ】** ・【TLS 1.0】【TLS 1.1】【TLS1.2】をチェック
4)信頼済みサイトに登録する	以下の項目に本 URL を設定します **→【ツール】→【インターネットオプション】** **→【セキュリティ】→【信頼済みサイト】→【サイト】** https://ccs01.deviceid.kddi.ne.jp
5)キャッシュをクリアする（任意）	以下の項目を有効にし削除します。 **→【ツール】→【インターネットオプション】** **→【全般】→【削除（閲覧の履歴）】** ・【インターネット一時ファイルおよびウェブサイトのファイル】をチェック

1.3 アクセス先 URL

証明書カスタマーコントロールの接続先 URL は、以下のとおりです。ブラウザから URL を入力すると、証明書カスタマーコントロールのログイン画面に移ります。

接続先 URL： https://ccs01.deviceid.kddi.ne.jp/

1.4 本システムでの用語の説明

本システムでは、以下の用語を利用します。

用語	解説
認証局（CA 局）	証明書の発行・失効・管理を行うサイバートラスト社設備です。
証明書	デバイスにインストールされる p12 形式の電子証明書です。
証明書の発行	電子証明書を、認証局に依頼し生成し発行を行います。発行された証明書は、メールにて通知されます。
証明書の失効	電子証明書を、認証局に依頼し失効を行います。失効された証明書は、CRL に記載され有効性を失います。
証明書の取得	端末から認証局にアクセスし専用アプリケーション、またはブラウザ(Windows®の場合)、OTA(Over The Air)(iOS の場合)にて証明書をダウンロードする行為です。 各端末にて操作を行いますと、証明書の取得インストールまでが一連の動作として行われます。 ※ OTA とは、iOS にて具備されている無線(Wi-Fi/LTE)を利用してアプリケーション、構成プロファイルなどをインストール可能とする機能です。
格納ストア	Windows®の証明書配置場所を表します。コンピューターストアは、全ユーザー共通で利用されるストアを表します。ユーザーストアはログインユーザーのみが参照可能なストアとなります。 **【重要】「KDDI FRE」でコンピューターストア証明書を利用する場合は、オプション申込を行った上でご利用ください。**
取得方法	Windows®端末への証明書インストール方法を表します。 Importer：専用ソフトウエアを利用する方法です。 Active X：ブラウザ経由で Active X を利用する方法です。
通知先メールアドレス	証明書の発行通知、取得可否変更などを通知する先のメールアドレスです。
構成プロファイル	iOS デバイスを設定するための XML 形式のファイルです。 OTA(Over The Air)により証明書と同時に配布されます。 **【重要】「KDDI FRE」にて『Cisco AnyConnect』を利用するためには構成プロファイルを適用して証明書を発行することが必要です。**

<table>
<tr><td>Common Name(CN)</td><td>証明書に記載された、証明書を識別する値で、【お客さま設定値(ID 箇所)】@【お客さまご契約の suffix 名】の形式となります。本システム上では重複した値を設定することも可能ですが、ログイン履歴調査などを円滑に実施するためユニークにしてください。
なお、『オンデマンド接続』『Always-On 接続』では、本 CN 値にて同時接続制限を行いますので、重複した値を設定する場合にはご注意いただきますようお願いします。</td></tr>
<tr><td>Auth ID 種別</td><td>端末を識別する情報(Auth ID)の種類を表します。

Windows(R)の場合:MAC アドレスを利用できます。
Android(TM)の場合:MAC アドレス/IMEI どちらかを利用できます。
※Android™10 以降は MAC アドレスのみ利用できます。
iOS の場合:IMEI/UDID のどちらかを利用できます。
MAC OS の場合:MAC アドレスを利用できます。
Windows® Mobile の場合:GUID を利用できます。

【重要】UDID 値の入手は、Apple 社ツールをご利用いただく必要があります。
※ iPadOS をご利用の場合は『iOS』を選択ください</td></tr>
<tr><td>Auth ID</td><td>端末を識別する固有の情報を表します。</td></tr>
<tr><td>UPN</td><td>User Principal Name の略。Active Directory ドメインの環境でユーザーを一意に識別できます。</td></tr>
<tr><td>ポリシ ID</td><td>発行する証明書に適用される情報です。OS ごとに値を選択する必要があります。本システムでは、ポリシ ID 値に基づき発行通知メール本文などが変更になります。</td></tr>
<tr><td>署名アルゴリズム</td><td>デジタル署名に用いるアルゴリズム(ハッシュ関数の種類)を表します。</td></tr>
<tr><td>認証局</td><td>認証局の世代を表します。
<table>
<tr><th>名称</th><th>説明</th><th>署名アルゴリズム</th></tr>
<tr><td>G1</td><td>2014 年 3 月 24 日以前に KDDI へ申請された証明書を管理している認証局</td><td rowspan="2">SHA-1</td></tr>
<tr><td>G2</td><td rowspan="2">証明書カスタマーコントロール(本システム)から発行した証明書を管理している認証局</td></tr>
<tr><td>G3</td><td>SHA-2(256)</td></tr>
</table>
</td></tr>
</table>

2 証明書の管理・運用方法

2.1 証明書管理の概要

証明書の発行から失効まで、一般的な証明書の管理方法について、管理者さまが行うことは以下のようになります。(下線部は本システムで実施する箇所)

端末の運用フェーズ	管理者さまが行うこと (本マニュアルでの参照先)	利用者さまが行うこと
1 利用準備 (証明書インストールまで)	**利用端末の固有情報(Auth ID)の取得** ・Windows®、MAC OS: MAC アドレス ・iOS: IMEI または UDID ・Android™: IMEI または MAC アドレス ※Android™10 以降は MAC アドレスのみ ・Windows® Mobile:GUID	(必要に応じて) 端末固有情報の確認・連絡
	証明書の発行通知メールの宛先となる**メールアドレス情報の取得**	(必要に応じて) メールアドレスの連絡
	(iOS デバイスで「KDDI FRE」へ接続する場合) **構成プロファイルの作成・登録**(7 章)	
	証明書の発行申請(4 章) Auth ID、メールアドレス、構成プロファイル(iOS の場合のみ)を使用して発行	発行通知メール受信後、証明書インストール
	(証明書インストール可能な期間にインストールできなかった場合) **証明書の取得可否変更**(6.2 章)により、証明書を再度取得可能な状態に変更	再取得可能な通知メール受信後、証明書インストール
2 端末利用中 (証明書インストール後)	(端末利用者の変更などで通知メールの宛先を変更する場合) **通知メールの宛先を一括で変更**(6.4 章)	
	(iOS デバイスで構成プロファイルを変更する場合) 新しい構成プロファイルを登録し、更新対象の端末を指定して**構成プロファイルの変更を申請**(7.3 章、7.8 章)	構成プロファイルの変更通知メール受信後、新しい構成プロファイルをインストール(上書き)

	（有効期間の満了前に証明書を更新する場合） **新規に証明書の発行申請（4 章）**を行い、インストール後、**古い証明書の失効を申請（5 章）**	発行通知メール受信後、証明書インストール 旧証明書、プロファイルの削除を推奨
3.端末利用終了時	（紛失など個々の端末利用を終了する場合） 対象の**証明書の失効申請（5 章）**	
4. 端末更新時	（新しい端末に変更する場合） 新しい端末向けに**新規に証明書の発行申請（4 章）**を行い、古い端末の**証明書の失効を申請（5 章）**。	発行通知メール受信後、新しい端末にて証明書インストール

2.2 証明書のステータスについて

証明書のステータスの遷移について説明します。

・証明書の発行から失効までのステータス

証明書の発行申請を行った後、認証局にて発行されると『発行済み』のステータスとなります。また、証明書の失効申請を行った後、認証局にて失効されると『失効済み』のステータスとなります。

『有効な証明書』は、『発行済み』のステータスの証明書となり、課金対象となります。（『失効済み』の証明書は非課金対象）

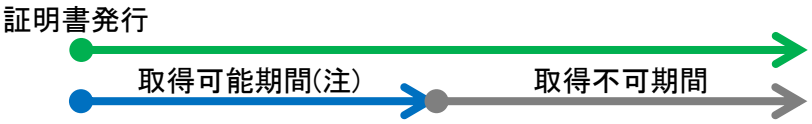
なお、一度失効した証明書を再度有効にすることはできません。必要な場合は新たに証明書を発行し、端末にインストールします。

ステータス	発行済み	失効済み
有効な証明書	●（有効）	×（有効でない）
課金対象	●（課金対象）	×（非課金対象）
サービス利用	●（利用可能）	×（利用不可）

・証明書の取得可否のステータス

認証局にて証明書が発行されると、利用者さまへ発行通知メールが送信され、証明書を取得(インストール)可能になります。ただし、一定期間を経過するとセキュリティ上、取得が不可能になります(認証局のサーバー側でロックがかかります)。

取得不可能になった証明書は、管理者さまによる『取得可否変更』操作を行うことで、再度取得可能な状態になります。(再取得可能になると、利用者にはメールで通知されます)



取得可否状態	取得可能	取得不可
有効な証明書	●(有効)	
課金対象	●(課金対象)	
サービス利用	●(利用可能)	

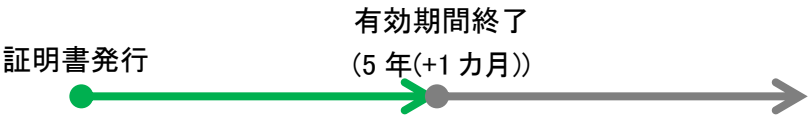
注) 取得可能期間:証明書発行日から 7 日間、
または証明書の初回ダウンロード日から 3 日間
(『取得可否変更』操作後の取得期限も同様)

・証明書の有効期間

証明書には有効期間があり、発行した日時から 5 年(+1 カ月)間となります。

有効期間が終了した証明書は利用できません(認証されません)ので、必要な場合は新規に証明書を発行してインストールします。

有効期間が終了した証明書は非課金対象となります。また、『失効』や『取得可否変更』の操作は行えなくなります。



ステータス	発行済み	有効期間終了
有効な証明書	●(有効)	×(有効でない)
課金対象	●(課金対象)	×(非課金対象)
サービス利用	●(利用可能)	×(利用不可)

2.3 発行/失効申請処理時間

証明書の発行/失効申請後、最短で 5 分程度で処理が完了し、発行申請の場合は通知メールが端末へ送信されます。

※ 一括発行申請の場合、CSV ファイルの行数により処理時間が増大します。500 枚同時発行時の目安は最短で 1 時間程度になります。

※ 認証局側の処理はほかのお客さまの申請に対してシリアルに処理が行われる関係で、ほかのお客さま申請による待ち時間があります。

2.4 機能一覧

本カスタマーコントロールシステムでは以下の機能をご利用可能です。

大項目	中項目	機能概要
証明書の発行申請	証明書の発行申請	証明書を 1 枚単位で発行可能です。
	証明書の一括発行申請	証明書を複数枚一括で発行可能です。
証明書の失効申請	証明書の失効申請	証明書を 1 枚単位もしくは複数一括で失効可能です。
	証明書の一括失効申請	証明書を 1 枚単位もしくは複数一括で失効可能です。
証明書の管理	申請情報の検索	過去に申請された証明書に関わるデータを参照可能です。また、一括申請データフォーマットとしてダウンロード可能です。
	証明書の取得可否変更	証明書のダウンロード可否の変更が可能です。
	通知用アドレス一括変更	証明書発行時にメール通知するメールアドレスの一括変更が可能です。
構成プロファイルの管理	構成プロファイルの登録・削除	iOS デバイス向け構成プロファイルの管理が可能です。 **【重要】「KDDI FRE」にて『Cisco AnyConnect』(iOS 版)を利用するためには構成プロファイルが必要です。**
	構成プロファイルの簡易作成	iOS デバイス向け構成プロファイルの作成が可能です。 **【重要】「KDDI Flex Remote Access」サービス利用者のみ利用可能です。**
	構成プロファイルの変更	iOS デバイス向け構成プロファイルの変更が可能です。 **【重要】2014 年 3 月 24 日以前に発行された証明書に構成プロファイルを適用している場合、変更処理が動作しません。構成プロファイル内容を変更したい場合、新たに発行・インストールした後、古い証明書を失効いただく必要があります。**

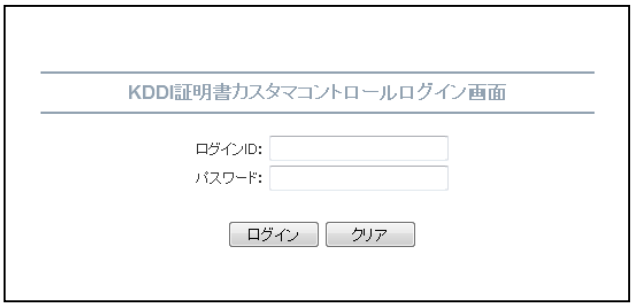
レポートの出力	証明書のレポート	直近 6 カ月の証明書情報を検索・取得可能です。
	証明書のサマリレポート	直近 6 カ月の証明書サマリ情報を検索・取得可能です。
監査	ログの検索	管理者さまによる各操作の履歴を検索することが可能です。
管理者アカウント	パスワードの変更	管理者さまによるパスワード変更が可能です。
	証明書有効期間終了の事前通知設定	直近 3 カ月にて証明書有効期間終了となる契約について、通知メールの送信先メールアドレスの登録が可能です。
オンライン・ヘルプ	マニュアル	証明書カスタマーコントロールマニュアルページへリンクします。
	お知らせ	予定される定期メンテナンス情報を掲載します。

3　ログイン操作

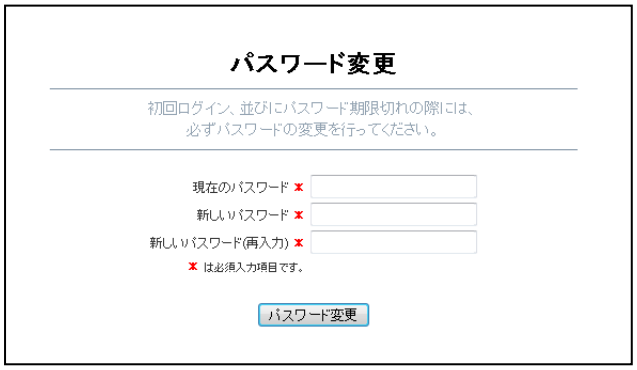
3.1　初回ログイン

前述の URL へアクセスし、『証明書カスタマーコントロール開通のご案内』に記載または、『契約管理システム』(契約内容照会)に表示されているログイン ID と初期パスワードを入力します。

初回ログイン時には、初期パスワードを変更する必要があります。



ログイン ID と初期パスワードを入力します。



初回ログイン時は、必ずパスワードの変更が必要です。

管理者アカウントのログインパスワードの文字制限事項は、以下のとおりです。

・半角英数文字（記号は利用不可）8 文字以上、16 文字以内

・英字と数字の混在必須

・ログイン ID と同値、現在のパスワードと同値は利用不可

3.2　2 回目以降のログイン

2 回目以降のログインについては、ログイン ID とパスワードを入力することでシステム操作を開始できます。

3.3　パスワードロック

3 回パスワード入力を間違えるとパスワードロックがかかります。

パスワードロックが発生した場合、『14 お問い合わせ窓口』に記載している KDDI 窓口(KDDI サービスコントロールセンター(SCC))までロック解除依頼のご連絡いただくようお願いします。

3.4　トップ画面

ログイン後のトップ画面は以下のようなイメージです。

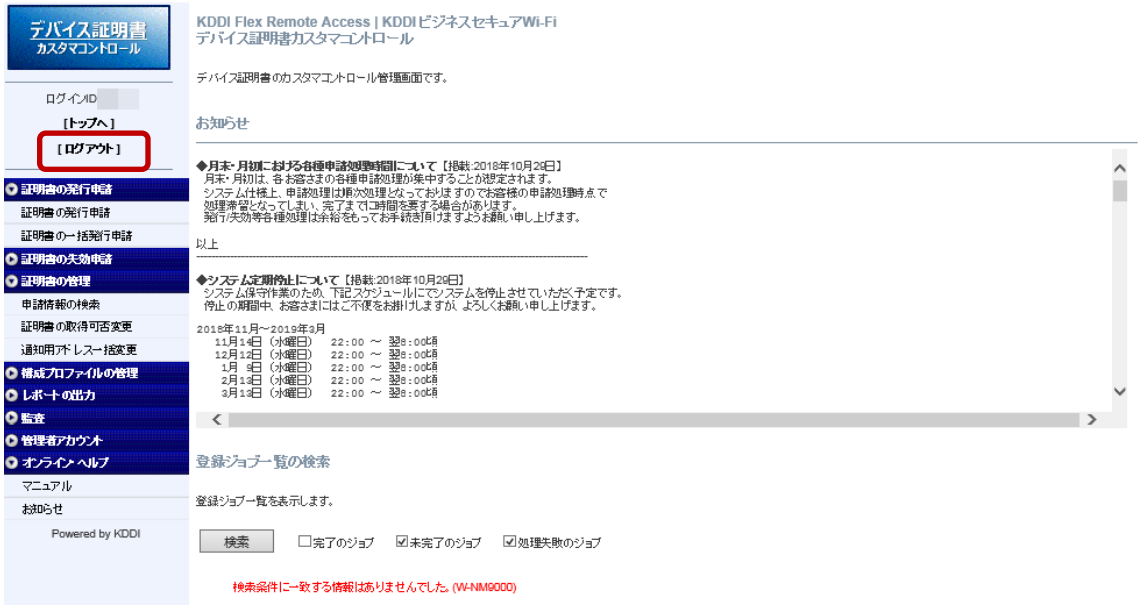
画面は左側フレームに操作メニューが並び、右側フレームに操作実施領域および結果表示領域が配置されます。

右側フレームには、システムメンテナンスによる停止日時などのお知らせ情報および、前回までに処理が行われた各種申請結果の内 NG となったものが表示されます。『トップへ』を押下すると本画面に戻ります。

※ 認証局に対する処理は、1 つずつの処理に『ジョブ』と呼ばれる通番が割り当てられ管理されます。すべての『ジョブ』にはタイムアウト時間が設けられており、認証局の処理遅延などにより処理 NG(エラー)となる場合があります。

3.5 ログアウト操作

ログアウト操作は、メニュー領域の『ログアウト』より実施します。



ブラウザの『×』ボタンにより閉じた場合セッションが残り、最大 30 分程度ログインが不可となります。

もし『×』ボタンによりブラウザを閉じてしまった場合は、時間をおいて再ログインしてください。

なお、本システムでは同時接続を 2 つまで許容しています。ログインしているユーザーがログアウトを行わずにブラウザを終了させてしまった場合、このログイン情報が残ってしまうため、本システムの利用を終了する場合には、必ずログアウトしてください。ログアウトせずにブラウザを 2 回終了させてしまいログインができなくなった場合は、タイムアウト(最大 30 分程度)によりログアウト状態になるのを待ってから、再度ログインしてください。

4　証明書の発行申請

4.1　「KDDI FRE」で iOS/iPadOS デバイスをご利用のお客さま

App Store にて以下 2 つの AnyConnect アプリケーションが Cisco 社より提供されております。(2019 年 12 月現在)

Cisco Legacy AnyConnect 	旧来のAnyConnectから名称を変更 (従来の「KDDI FRE」で利用)	Ver.4.0.05069
Cisco AnyConnect 	新しいAnyConnect	Ver.4.0.07077～

iOS/iPadOS デバイスをご利用の場合は『Cisco AnyConnect』にて証明書を利用するために『iOS 構成プロファイル』を適用して証明書を発行する必要があります。そのため、**証明書発行申請前に『構成プロファイルの管理』メニューにて構成プロファイルを登録してください。**

ご利用デバイスの OS (利用する AnyConnect)	証明書発行時の構成プロファイルの適用	証明書発行手順	参照先
iOS/iPadOS (Cisco AnyConnect)	**必須**	**構成プロファイルの登録後、証明書の発行申請**	7 章 4 章
iOS/iPadOS (Cisco Legacy AnyConnect)	**推奨**	**構成プロファイルの登録は任意**	(7 章) 4 章
Windows®	不要	証明書の発行申請	4.2 から
MAC OS	不要	証明書の発行申請	4.2 から
Android™	不要	証明書の発行申請	4.2 から

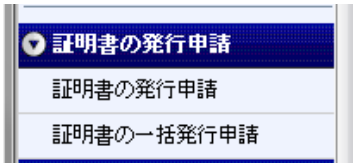
※ 利用者さま向けの『VPN 接続手順・VPN クライアントソフト操作マニュアル』では、『**Cisco AnyConnect**』のインストール手順を案内しております。『**Cisco Legacy AnyConnect**』(将来終了予定)を利用する場合は利用者さまへご案内ください。

※ 従来より『**Cisco Legacy AnyConnect**』をご利用のお客さまは構成プロファイルの適用は必須ではありませんが、将来的に『Cisco Legacy AnyConnect』は Cisco 社にて終了の計画があるため、構成プロファイルの利用または、『Cisco AnyConnect』のご利用(移行)をご検討ください。

※ 『Cisco AnyConnect』と『Cisco Legacy AnyConnect』の違い、移行方法については、『Cisco AnyConnect のご利用と移行方法について』を参照してください。
リモートアクセスサービス各種マニュアルページ
http://www.kddi.com/business/cpa_ccs/

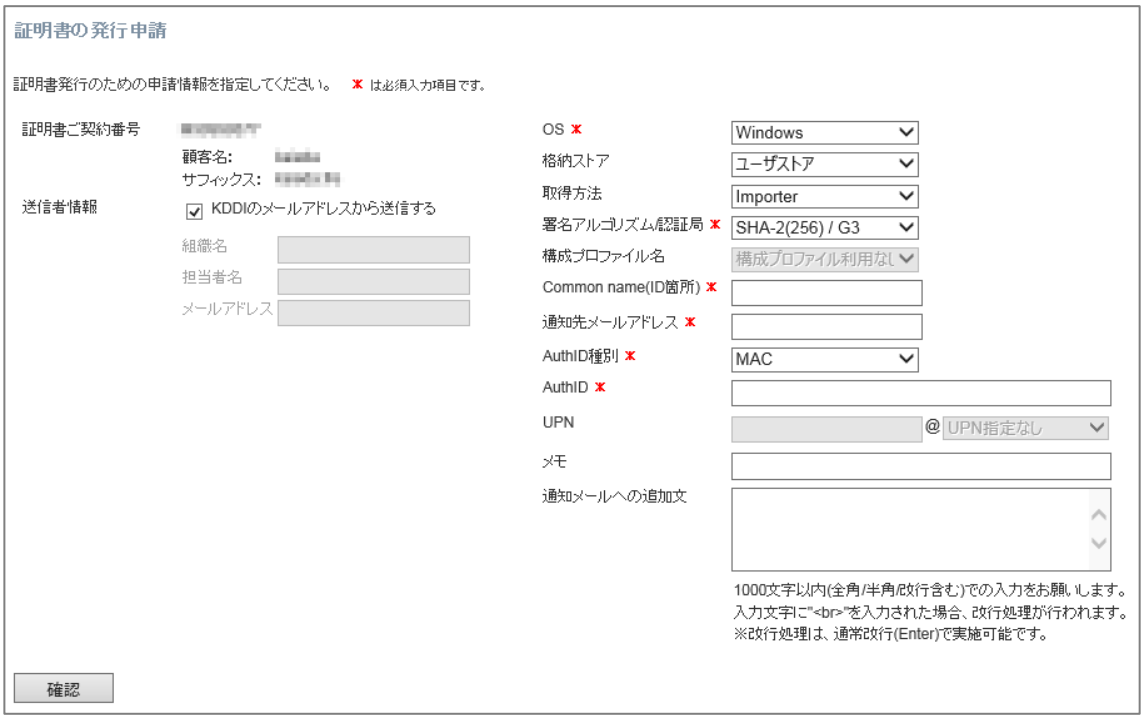
4.2　証明書の発行申請メニュー

メニューより【証明書の発行申請】を選択すると以下のように発行申請メニューが表示されます。



4.3　証明書の発行申請

証明書の発行申請では、1 枚ごとに証明書発行が可能となります。



各項目に選択もしくは入力が必要となります。必須項目を入力いただいたのちに【確認】ボタンをクリックしてください。

なお、【格納ストア】は、OS にて『Windows』を選択している場合のみ、『ユーザーストア』または『コンピューターストア』を選択可能です。【構成プロファイル名】は【OS】にて『iOS』を選択している場合のみ選択可能です(構成プロファイルを登録完了している場合のみ選択可能です)。

入力項目が不正であった場合、【確認】ボタンをクリックするとエラーが表示されます。

※ Android™10 向けに証明書を発行する場合、AuthID 種別は「MAC アドレス」をご選択ください。AuthID 種別で「IMEI」を選択し発行されても、IMEI 情報の取得が OS 制限により不可となったため、IMEI を利用した証明書発行/インストールができません。(Android™10 以降での仕様変更)

※ Android™10 に関して、AuthID 種別「MAC アドレス」をご利用の場合、端末側で事前に設定変更を実施いただく必要があります。MAC アドレスに関する情報をインストール用アプリケーションが取得する際に、ランダムな値となるのが初期仕様となっております(Android™10 以降での仕様変更)。そのため、事前に MAC アドレス情報を取得する際にはランダムな MAC アドレスではなく実際の MAC アドレスを固定的に返すように端末の設定を変更していただく必要があります。設定変更方法の詳細は、『証明書インストールマニュアル Android(TM)版』をご参照ください。

リモートアクセスサービス各種マニュアルページ
http://www.kddi.com/business/cpa_ccs/

【各入力項目の説明】

項目	方式	内容
送信者情報	選択 もしくは 入力	発行通知メール送信時に利用されるメールアドレスおよびメール署名欄の情報です。『KDDI のメールアドレスから送信する』を選択すると KDDI の送信専用メールアドレス『no-reply@deviceid.kddi.ne.jp』より発行通知メールを送付します。管理者さまの情報で証明書発行通知メールを送る場合は、チェックをはずし、『組織名』『担当者名』『メールアドレス』に管理者さま情報を入力します。詳しくは『13.1 メールフォーマット』をご参照ください。 **【重要】『KDDI のメールアドレスから送信する』のチェックをはずし、お客さまを指定される場合、メールアドレスは実在するものをご入力ください。** また、発行通知メールの不達時は、通常ここで設定したメールアドレスにエラーメールが返信されますので、管理者さまにて検知が必要な場合は、お客さまのメールアドレスに変更してください。また、存在しないメールアドレスを設定しないようご注意ください。

OS	選択	証明書を発行する OS を選択します。現在選択可能な OS は、Windows®/Windows® Moble /MAC OS/Android™/iOS となります。 iPadOS の場合は『iOS』、 Windows® パソコンの場合は『Windows』、 Windows® 10 Mobile の場合は『Windows Mobile』を選択してください。
格納ストア	選択	OS にて『Windows』を選んだ場合のみ選択可能です。ユーザーストア/コンピューターストアから選択できます。 **【重要】「KDDI FRE」でコンピューターストア証明書を利用する場合は、オプション申込を行った上でご利用ください。**
取得方法	選択	OS にて『Windows』を選んだ場合のみ選択可能です。『Importer』『Active X』から選択できます。 **【重要】クライアント環境により Active X が動作せず、証明書インストールができないお客さまは、Importer を選択ください。**(Importer: 証明書インストール専用アプリケーション)
署名アルゴリズム/認証局	選択	署名アルゴリズムと認証局を選択可能です。『SHA-1/G2』『SHA-2(256)/G3』から選択できます。**セキュリティとしては『SHA-2(256)』をおすすめします。**
構成プロファイル名	選択	OS にて iOS を選んだ場合のみ選択可能です。後述する構成プロファイルの管理にて事前登録した構成プロファイルから選択することができます。 本設定を実施することで証明書と iOS 構成プロファイルを同時配布します。 **【重要】『Cisco AnyConnect』(iOS 版)をご利用の場合、設定は必須になります。** **設定がない場合、『Cisco AnyConnect』が証明書を認識せず、「KDDI FRE」にて認証が行えません。**
Common name (ID 箇所)	入力	証明書内の CN 値に相当する値を入力いただきます。入力した値に対して自動的にシステムによりお客さま契約 suffix 情報を付与して証明書発行となります。CN の形式としては、【本項目の値】@【お客さまご契約の suffix 名】となります。 本システム上では重複した値を設定することも可能ですが、ログイン履歴調査などを円滑に実施するためユニー

		クにしてください。 なお、『オンデマンド接続』『Always-On 接続』では、本 CN 値にて同時接続制限を行いますので、重複した値を設定する場合にはご注意いただきますようお願いします。
通知先メールアドレス	入力	証明書発行通知メールの送付先を入力いただきます。メールの宛先になるのでタイプミスにご注意ください。
Auth ID 種別	選択	選択した OS 種別により選択項目が変わります。 Windows(R)の場合:MAC アドレス Windows(R) Mobile の場合:GUID Android(TM)の場合:IMEI または MAC アドレス ※Android™10 以降は MAC アドレスのみ iOS の場合:IMEI または UDID MAC OS の場合:MAC アドレス
Auth ID	入力	選択した Auth ID 種別により入力形式が変わります。 【MAC を選択している場合】 xx:xx:xx:xx:xx:xx 形式(半角) 【IMEI を選択している場合】 15 桁の半角数字 ※iOS 端末で IMEI が複数ある場合、主回線の IMEI のみご利用いただけます。 【UDID を選択している場合】 40 桁の半角英数字 または 25 桁の半角英数字(9 桁目にハイフンの区切り文字を含む) 【GUID を選択している場合】 Cybertrust DeviceiD Importer アプリケーション(Windows® 10 Mobile 版)で取得した 32 文字の半角英数字
UPN	入力・選択	証明書フィールドに UPN(User Principal 名)を出力する場合に利用します（「KDDI FRE」「KDDI ビジネスセキュア Wi-Fi」以外でも証明書を利用する場合で、かつ Active Directory 環境で証明書を利用する場合など)。 ご利用には別途お申し込みを行い、UPN サフィックス名(@以降の部分)はお申し込みいただいた文字列から選択します。

		UPN は次の証明書の場合に設定可能です。 ・Windows®：ユーザーストア、かつ Importer 指定時 ・iOS ・Android™ ・Windows® 10 Mobile
メモ	入力	証明書発行対象などの情報メモ欄(入力は任意)
通知メールのへの追加文	入力	証明書発行通知メール本文へ追加できる自由記述欄（入力は任意） 最大 1,000 文字（全角/半角/改行含む）まで入力可能です。入力文字に" "を入力された場合、改行処理が行われます。 ※ 証明書発行通知メール本文への追加イメージは『13.1 メールフォーマット』をご参照ください。

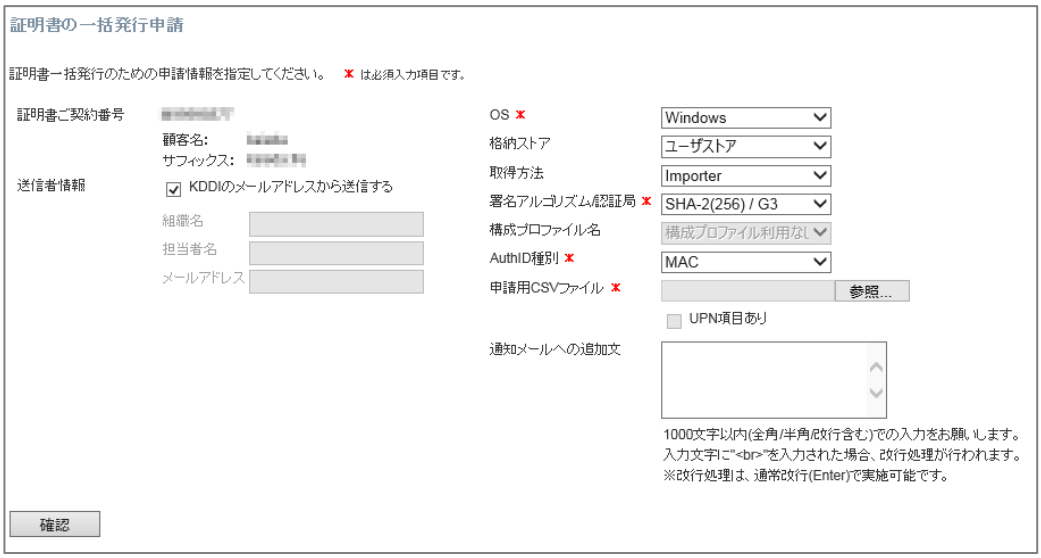
【注意】Windows® Mobile 向けの証明書認証において、端末側に複数の証明書が存在した場合、Cisco AnyConnect for Windows 10 Mobile(4.1.03017)では証明書の自動選択となるために正しい証明書を選択できず、この場合「KDDI FRE」に接続できません。

【エラーメッセージ例】

エラー表示	エラー内容
メールアドレスの書式が不正です。(W-DT1109)	送信者情報のメールアドレス形式が正しくない場合に表示されます。
Common name(ID 箇所)の文字数は 1 文字以上 15 文字以下で入力してください。(W-DT1111)	Common name に入力した値が文字数制限を超えている場合に表示されます。
Common name(ID 箇所)には半角数字、英小文字のみで入力してください。(W-DT1112)	Common name に半角数字・英小文字以外の記号や全角文字などが入っている可能性があります。
通知用メールアドレス書式が不正です。(W-DT1115)	発行通知するメールアドレス形式が正しくない場合に表示されます。
AuthID が MAC アドレスの書式と異なります。(W-DT1117)	MAC アドレスの書式が xx:xx:xx:xx:xx:xx 形式(半角)ではない可能性があります。
AuthID が IMEI の書式と異なります。(W-DT1118)	IMEI の書式が 15 桁の半角数字でない可能性があります。
AuthID が UDID の書式と異なります。(W-DT1119)	UDID の書式が 40 桁の半角英数字または 25 桁の半角英数字(9 桁目にハイフンの区切り文字を含む)でない可能性があります。
組織名が未入力です。(W-DT1003)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、組織名が入力されていません。
担当者名が未入力です。(W-DT1005)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、担当者名が入力されていません。
メールアドレスが未入力です。(W-DT1007)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、メールアドレスが入力されていません。

4.4　証明書の一括発行申請

証明書の一括発行申請では、CSV 形式フォーマットでファイルをアップロードすることにより証明書を一括発行します。



各項目に選択もしくは入力が必要となります。必須項目を入力いただいたのちに CSV ファイルをアップロードし確認ボタンをクリックしてください。

なお、【格納ストア】は OS にて『Windows』を選択している場合のみ、『ユーザーストア』/『コンピューターストア』を選択可能です。【構成プロファイル名】は OS にて iOS を選択している場合のみ選択可能です(事前に構成プロファイルの登録を完了している場合のみ表示され、選択が可能です)。

また、「KDDI FRE」「KDDI ビジネスセキュア Wi-Fi」以外で証明書をご利用される場合などで、UPN をご利用の場合は、別途 UPN ご利用のお申し込みの上、画面【UPN 項目あり】のチェックボックスを入れて所定フォーマットの CSV ファイルをアップロードしてください。

※【UPN 項目あり】の場合は CSV ファイルフォーマットが通常と異なります。

CSV ファイルにエラーレコードが存在する場合、【確認】ボタンをクリック後エラー表示されます。

【各入力項目の説明】

項目	方式	内容
送信者情報	選択 もしくは 入力	発行通知メール送信時に利用されるメールアドレスおよびメール署名欄の情報です。『KDDI のメールアドレスから送信する』を選択すると KDDI の送信専用メールアドレス『no-reply@deviceid.kddi.ne.jp』より発行通知メールを送付します。管理者さまの情報で証明書発行通知メールを送る場合は、チェックをはずし、『組織名』『担当者名』『メールアドレス』に管理者さま情報を入力します。詳しくは『16.1 メールフォーマット』をご参照ください。 **【重要】『KDDI のメールアドレスから送信する』のチェックをはずし、お客さまを指定される場合、メールアドレスは実在するものをご入力ください。** また、発行通知メールの不達時は、通常ここで設定したメールアドレスにエラーメールが返信されますので、管理者さまにて検知が必要な場合は、お客さまのメールアドレスに変更してください。また、存在しないメールアドレスを設定しないようご注意ください。
OS	選択	証明書を発行する OS を選択します。現在選択可能な OS は、Windows®/Windows® Mobile/ MAC OS/Android™/iOS となります。 iPadOS の場合は、『iOS』 Windows® パソコンの場合は、『Windows』 Windows® 10 Mobile の場合は、『Windows Mobile』を選択してください。
格納ストア	選択	OS にて『Windows』を選んだ場合のみ選択可能です。ユーザーストア/コンピューターストアから選択できます。 **【重要】「KDDI FRE」でコンピューターストア証明書を利用する場合は、オプション申込を行った上でご利用ください。**
取得方法	選択	OS にて『Windows』を選んだ場合のみ選択可能です。『Importer』『Active X』から選択できます。 **【重要】クライアント環境により Active X が動作せず、証明書インストールができないお客さまは、Importer を**

		選択ください。(Importer: 証明書インストール専用アプリケーション)
署名アルゴリズム/認証局	選択	署名アルゴリズムと認証局を選択可能です。『SHA-1/G2』『SHA-2(256)/G3』から選択できます。**セキュリティとしては『SHA-2(256)』をおすすめします。**
構成プロファイル名	選択	OS にて iOS を選んだ場合のみ選択可能です。後述する構成プロファイルの管理にて事前登録した構成プロファイルから選択することができます。 本設定を実施することで証明書と iOS 構成プロファイルを同時配布します。 **【重要】『Cisco AnyConnect』(iOS 版)をご利用の場合、設定は必須になります。 設定がない場合、『Cisco AnyConnect』が証明書を認識せず、「KDDI FRE」にて認証が行えません。**
Auth ID 種別	選択	選択した OS 種別により選択項目が変わります。 Windows(R)の場合:MAC アドレス Windows(R) Mobile の場合:GUID Android(TM)の場合:IMEI または MAC アドレス ※Android™10 以降は MAC アドレスのみ iOS の場合:IMEI または UDID MAC OS の場合:MAC アドレス
申請用 CSV ファイル	アップロード	別途お客さまによるご用意いただく CSV ファイルをアップロードいただきます。CSV ファイルのフォーマットについては、『13.2 各種申請 CSV フォーマット』をご参照ください。
通知メールのへの追加文	入力	証明書発行通知メール本文へ追加できる自由記述欄（入力は任意） 最大 1,000 文字（全角/半角/改行含む）まで入力可能です。入力文字に" "を入力された場合、改行処理が行われます。 ※ 証明書発行通知メール本文への追加イメージは『13.1 メールフォーマット』をご参照ください。

※ CSV ファイルの行数により処理時間が変動します。

※ ほかのお客さまの申請状況によっては発行完了までに数時間を要する場合があります。

【申請用 CSV エラーメッセージ例】

エラー表示	エラー内容
申請用 CSV ファイルの Common name(ID 箇所)には半角数字、英小文字のみで入力してください。(x 行目)(W-DT1016)	Common name に半角数字・英小文字以外の記号や全角文字などが入っている可能性があります。
申請用 CSV ファイルのメールアドレス書式が不正です。(x 行目)(W-DT1019)	発行通知するメールアドレス形式が正しくない場合に表示されます。
申請用 CSV ファイルの AuthID が MAC アドレスの書式と異なります。(x 行目)(W-DT1021)	MAC アドレスの書式が xx:xx:xx:xx:xx:xx 形式(半角)ではない可能性があります。
申請用 CSV ファイルの AuthID が IMEI の書式と異なります。(x 行目)(W-DT1022)	IMEI の書式が 15 桁の半角数字でない可能性があります。
申請用 CSV ファイルの AuthID が UDID の書式と異なります。(x 行目)(W-DT1023)	UDID の書式が 40 桁の半角英数字または 25 桁の半角英数字(9 桁目にハイフンの区切り文字を含む)でない可能性があります。
申請用 CSV ファイルが未入力です。(W-DT1010)	CSV 形式ファイルがアップロードされていません。
申請用 CSV ファイルの Common name(ID 箇所)が未入力です。(x 行目)(W-DT1014)	特定行の Common name 欄が空白です。
申請用 CSV ファイルのメールアドレスが未入力です。(x 行目)(W-DT1017)	特定行の通知先メールアドレス欄が空白です。
申請用 CSV ファイルの AuthID が未入力です。(x 行目)(W-DT1020)	特定行の Auth ID 欄が空白です。
申請用 CSV ファイルのカラム数が不正です。(x 行目)(W-DT1012)	CSV フォーマットのカラムが足りません。

組織名が未入力です。(W-DT1003)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、組織名が入力されていません。
担当者名が未入力です。(W-DT1005)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、担当者名が入力されていません。
メールアドレスが未入力です。(W-DT1007)	送信者情報で『KDDI のメールアドレスから送信する』のチェックが外れていますが、メールアドレスが入力されていません。

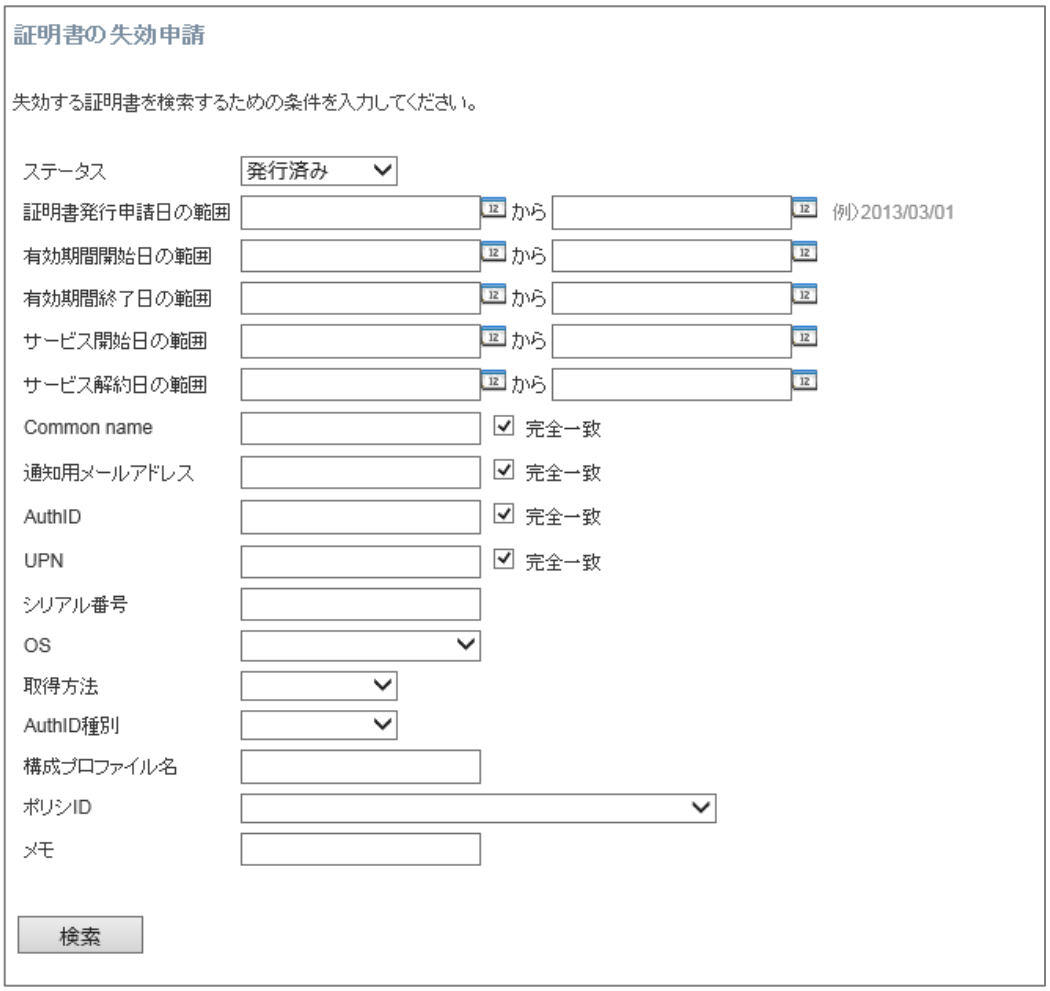
【注意】CSV ファイルの内部チェックを行う際に、最初のエラーが確認された段階でエラー表示されます。複数行に渡ってエラーがある場合も想定されますのでエラーが発生したら今一度記述内容をご確認ください。

5　証明書の失効申請

メニュー領域より証明書の失効申請を選ぶと以下のとおり失効申請メニューが表示されます。

5.1　証明書の失効申請

証明書の失効申請では、1 枚ごとに証明書の失効を行えます。



上記検索画面より失効対象の証明書を検索します。検索キーとしては以下の利用が可能です。

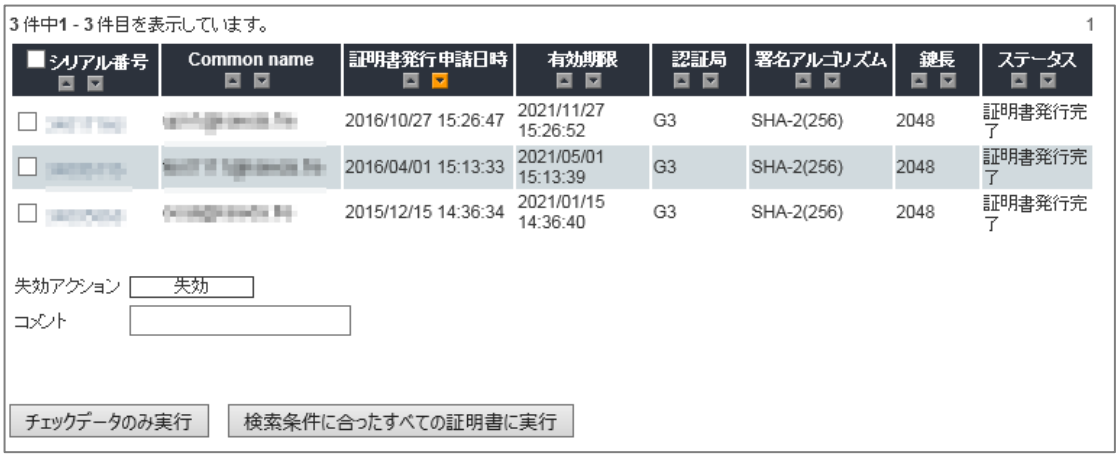
※ サービス開始日の範囲、サービス解約日の範囲はご利用になれません。

【検索キー】

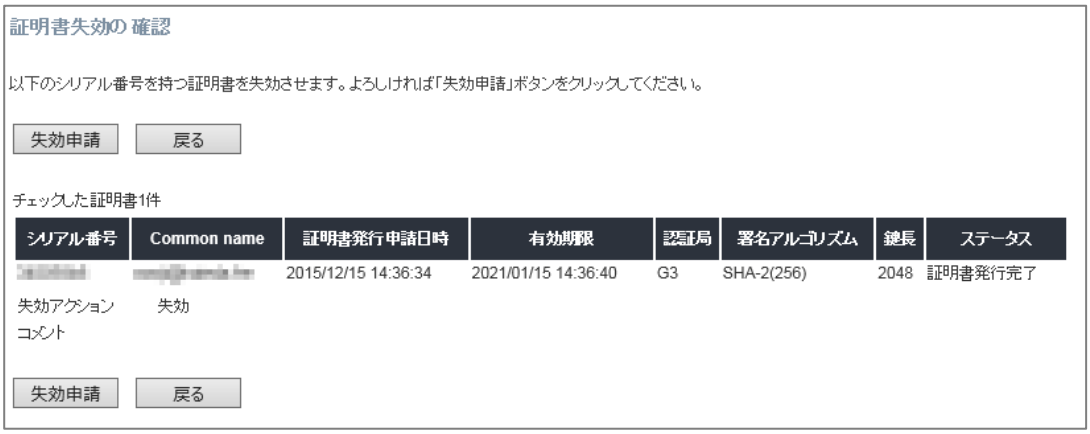
検索キー	内容
証明書発行申請日の範囲	証明書発行処理をした日付を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択できます。
有効期間開始日の範囲	証明書有効期間開始日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択できます。
有効期間終了日の範囲	証明書有効期間終了日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択できます。
Common name	証明書に設定された CN 値検索が利用可能です。完全一致検索を行う場合はお客さまご利用 suffix 情報を含む、『xxxx@yyy』のメールアドレス形式にて検索してください。
通知用メールアドレス	発行通知メール送付先メールアドレスから検索可能です。
Auth ID	端末の MAC アドレス/IMEI/UDID の情報から検索可能です。 【注意】2014 年 3 月 24 日以前に KDDI に申請書を送付して発行された証明書情報の内 Windows®端末分については、Hash 処理された値で検索する必要があります。
UPN	証明書発行時に UPN を指定した場合 UPN の値で検索可能です。
シリアル番号	証明書のシリアル番号から検索可能です。
OS	OS 種別より検索可能です。
取得方法	Importer/Active X から検索可能です。
AuthID 種別	MAC アドレス/IMEI/UDID/GUID の種別から検索可能です。
構成プロファイル名	iOS デバイスに適用している構成プロファイル名から検索が可能です。(部分一致)

	【注意】構成プロファイル名は、ほかのお客さまとのユニーク性を確保するため証明書発行後は KDDI 指定ルールで保存されます。完全一致での検索を実施する場合証明書詳細情報を確認いただき OU 値に含まれる"Profile"から始まる値を入力ください。
ポリシ ID	OS 種別+AuthID 種別での複合検索キーとして利用可能です。 以下プルダウンイメージから選択いただきます。  【注意】Android™用 AnyConnect 適用無は、KDDI に申請書を送付して発行された証明書の一部に適用されているポリシ ID です。本システムからの新規発行時にはご利用いただくことができません。
メモ	証明書発行時に記入したメモの値から検索が可能です。

各検索キー入力後、検索ボタンをクリックすることで該当する証明書が以下のイメージで下部に表示されます。



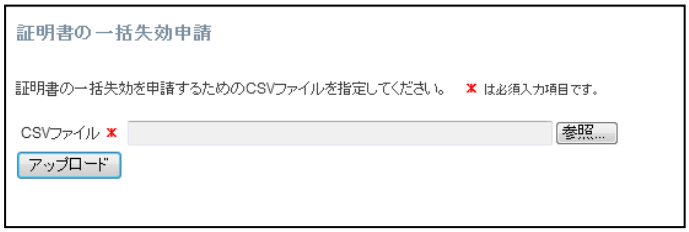
失効対象の証明書シリアル番号にチェックを入れ、チェックデータのみ実行をクリックするか、検索条件に合ったすべての証明書に実行をクリックすることで証明書失効確認画面が表示されます。



再度失効対象を確認して問題がなければ失効申請をクリックしてください。

5.2 証明書の一括失効申請

証明書の一括失効申請では、CSV 形式フォーマットでファイルをアップロードすることにより証明書を一括失効します。



失効申請用 CSV ファイルフォーマットについては、『13.2 各種申請 CSV フォーマット』をご参照ください。

※ CSV ファイルの行数により処理時間が変動します。

※ ほかのお客さまの申請状況によっては失効完了までに数時間を要する場合があります。

5.3　申請エラーについて

ステータスが『失効済み』の証明書に対して重複して失効申請/一括失効申請を行いますと、申請処理結果 NG となることがあります。失効申請対象の証明書を選択する際には、ご注意ください。

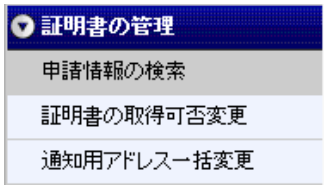
また、失効申請処理 NG となり、かつ証明書はステータス『発行済み』のままの場合は、課金対象となりますのでご留意ください。

※ 申請処理結果の確認手順については、『12. 各種処理状況の確認』をご参照ください。

※ 認証局に対して失効申請完了しているが、本システム画面上はステータス『発行済み』のままとなっている可能性がございます。失効申請処理結果 NG の場合、『6.3 証明書のステータスの更新』にて【再取得】を実行してください。

6　証明書の管理

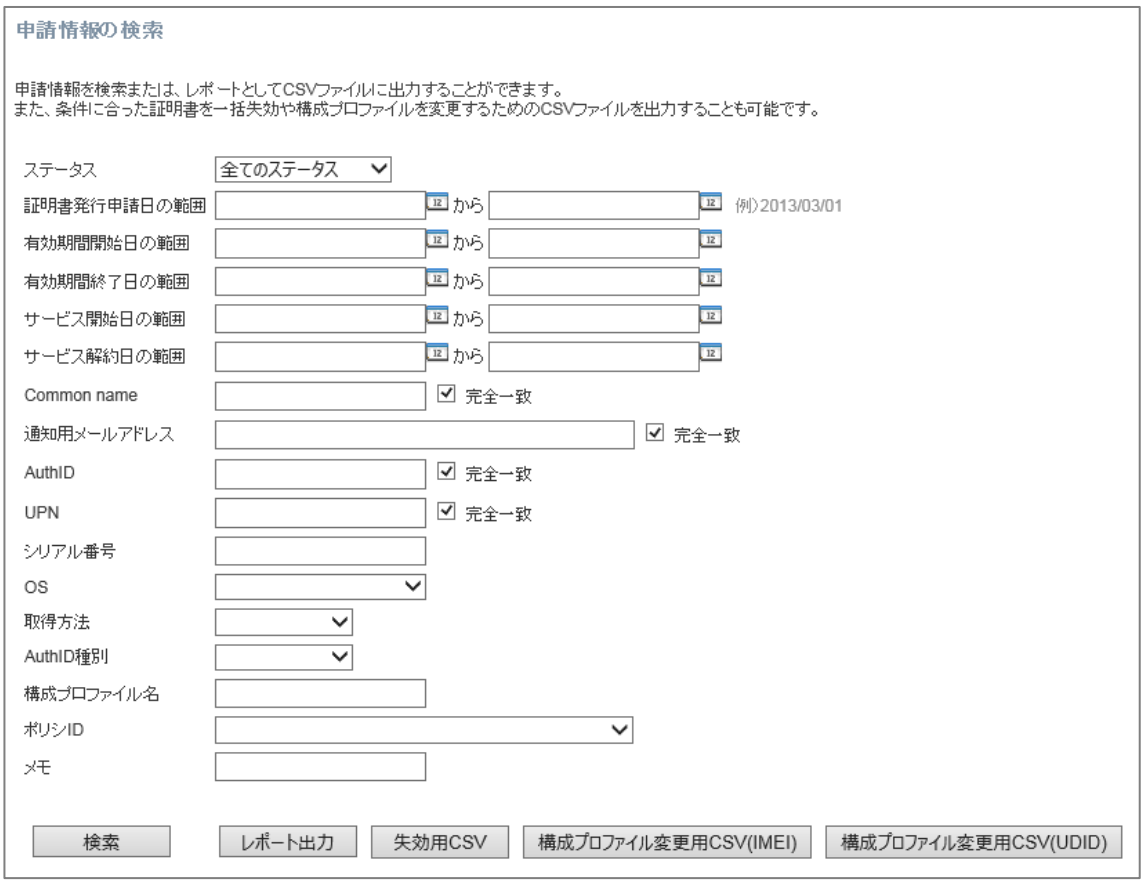
メニュー領域より証明書の管理を選ぶと以下のとおり管理メニューが表示されます。



6.1　申請情報の検索

申請情報の検索では、各種条件に基づき証明書の情報検索が可能となります。

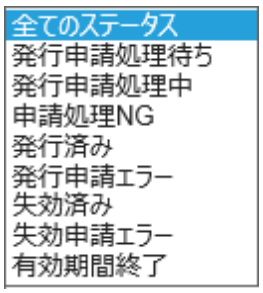
また申請情報検索結果より CSV 出力が可能です。



検索キーとしては以下の利用が可能です。

※ サービス開始日の範囲、サービス解約日の範囲はご利用になれません。

【検索キー】

検索キー	内容
ステータス	証明書申請に後の検索可能なステータスは以下のとおりです。 
証明書発行申請日の範囲	証明書発行処理をした日付を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間開始日の範囲	証明書有効期間開始日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間終了日の範囲	証明書有効期間終了日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
Common name	証明書に設定された CN 値検索が利用可能です。完全一致検索を行う場合はお客さまご利用 suffix 情報を含む、『xxxx@yyy』のメールアドレス形式にて検索してください。
通知用メールアドレス	発行通知メール送付先メールアドレスから検索可能です。
Auth ID	端末の MAC アドレス/IMEI/UDID の情報から検索可能です。 【注意】KDDI に申請書を送付して発行された証明書情報の内 Windows®端末分については、Hash 処理された値で検索する必要があります。
UPN	証明書発行時に UPN を指定した場合 UPN の値で検索可能です。

シリアル番号	証明書のシリアル番号から検索が可能です。
OS	OS 種別より検索が可能です。
取得方法	Importer または Active X から検索可能です。
AuthID 種別	MAC アドレス/IMEI/UDID/GUID の種別から検索可能です。
構成プロファイル名	iOS デバイスに適用している構成プロファイル名から検索が可能です。(部分一致) 【注意】構成プロファイル名は、ほかのお客さまとのユニーク性を確保するため証明書発行後は KDDI 指定ルールで保存されます。完全一致での検索を実施する場合証明書詳細情報を確認いただき OU 値に含まれる"Profile"から始まる値を入力ください。
ポリシ ID	OS 種別+AuthID 種別での複合検索キーとして利用可能です。 以下プルダウンイメージから選択いただきます。  【注意】Android™用 AnyConnect 適用無は、KDDI に申請書を送付して発行された証明書の一部に適用されているポリシ ID です。本システムからの新規発行時にはご利用いただくことができません。
メモ	証明書発行時に記入したメモの値から検索が可能です。

検索、CSV 出力ボタンについては以下のとおりです。

ボタン名	出力概要
検索	検索キーに基づき、検索結果が画面下部に表示されます。
レポート出力	検索キーに基づき、画面下部表示内容を CSV ファイルとして出力します。出力ファイル名は、 『証明書検索結果レポート_″yyyymmddhhmm″.csv』となります。
失効用 CSV	検索キーに基づき、一括失効申請用ファイルフォーマットとして出力します。出力ファイル名は、 『失効用リスト_″yyyymmddhhmm″.csv』となります。
構成プロファイル変更用 CSV(IMEI)	検索キーに基づき、構成プロファイル変更フォーマットとして出力します。出力ファイル名は、 『構成プロファイル変更リスト(IMEI)_″yyyymmddhhmm″.csv』となります。 IMEI での対象がない場合、出力ファイルは空ファイルとなります。
構成プロファイル変更用 CSV(UDID)	検索キーに基づき、構成プロファイル変更フォーマットとして出力します。出力ファイル名は、 『構成プロファイル変更リスト(UDID)_″yyyymmddhhmm″.csv』となります。 UDID での対象がない場合、出力ファイルは空ファイルとなります。

検索ボタンをクリックすると、以下のとおり検索結果が画面下部に表示されます。


10 件中1 - 10 件目を表示しています。 1

シリアル番号	Common name	証明書発行申請日時	有効期限	認証局	署名アルゴリズム	鍵長	ステータス
[redacted]	[redacted]	2016/10/27 15:26:47	2021/11/27 15:26:52	G3	SHA-2(256)	2048	証明書発行完了
[redacted]	[redacted]	2016/06/22 11:45:53	2021/07/22 11:45:58	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/22 11:42:16	2021/07/22 11:42:22	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/22 11:30:46	2021/07/22 11:30:52	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/01 15:47:26	2021/07/01 15:47:31	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/01 15:46:47	2021/07/01 15:46:53	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/01 15:46:08	2021/07/01 15:46:13	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/06/01 15:45:27	2021/07/01 15:45:31	G3	SHA-2(256)	2048	証明書の失効完了
[redacted]	[redacted]	2016/04/01 15:13:33	2021/05/01 15:13:39	G3	SHA-2(256)	2048	証明書発行完了
[redacted]	[redacted]	2015/12/15 14:36:34	2021/01/15 14:36:40	G3	SHA-2(256)	2048	証明書発行完了

検索結果の項目は以下のとおりです。

<table>
<tr><th>項目名</th><th>内容</th></tr>
<tr><td>シリアル番号</td><td>証明書ごとに固有なキーであるシリアル番号が表示されます。</td></tr>
<tr><td>Common name</td><td>証明書の Common Name が表示されます。</td></tr>
<tr><td>証明書発行申請日時</td><td>証明書発行申請された日時が表示されます。</td></tr>
<tr><td>有効期限</td><td>証明書の有効期限が表示されます。有効期限は発行日から 5 年(+1 カ月)です。</td></tr>
<tr><td>認証局</td><td>認証局の世代を表します。
<table>
<tr><th>名称</th><th>認証局世代</th><th>説明</th><th>署名アルゴリズム</th></tr>
<tr><td>G1</td><td>第 1 世代</td><td>2014 年 3 月 24 日以前に KDDI へ申請された証明書を管理している認証局</td><td rowspan="2">SHA-1</td></tr>
<tr><td>G2</td><td>第 2 世代</td><td rowspan="2">証明書カスタマーコントロール(本システム)から発行した証明書を管理している認証局</td></tr>
<tr><td>G3</td><td>第 3 世代</td><td>SHA-2(256)</td></tr>
</table></td></tr>
<tr><td>署名アルゴリズム</td><td>デジタル署名に用いるアルゴリズム(ハッシュ関数の種類)を表します。</td></tr>
<tr><td>鍵長</td><td>証明書における公開鍵長が表示されます。</td></tr>
<tr><td>ステータス</td><td>証明書の最終ステータスが表示されます。</td></tr>
</table>

【申請情報の詳細ページ】

各項目の内容は以下のとおりです。

項目名	内容
Common name	証明書の Common Name の値が表示されます。Common Name はお客さまによる指定したものとなります。
Organizational Unit	証明書の Organizational Unit の値が表示されます。Organizational Unit の値は認証局にて指定したものとなります。
Organization	証明書の Organization の値が表示されます。Organization の値は認証局または KDDI にて指定したものとなります。

<table>
<tr><td>Country</td><td>証明書の Country の値が表示されます。Country の値は認証局にて指定したものとなります。</td></tr>
<tr><td>リクエスト ID</td><td>認証局のリクエスト ID の値が表示されます。リクエスト ID は証明書の発行申請時にシステムから割り当てられるユニークな番号です。</td></tr>
<tr><td>バルク ID</td><td>証明書の発行申請の申請ごとにシステムから割り当てられる番号です。一括申請したものは同じ ID となります。</td></tr>
<tr><td>通知用メールアドレス</td><td>証明書の発行申請時に管理者さまが指定したメールアドレスが表示されます。発行通知や構成プロファイルの変更時などの通知メールの送信先になります。管理者さまによる変更可能な項目です。</td></tr>
<tr><td>シリアル番号</td><td>認証局にて割り当てられた証明書のシリアル番号の値が表示されます。シリアル番号は証明書をユニークに示す値となります。</td></tr>
<tr><td>有効期間の開始</td><td>証明書の有効期間の開始日時が表示されます。認証局が証明書を発行した日時となります。</td></tr>
<tr><td>有効期間の終了</td><td>証明書の有効期間の終了日時が表示されます。認証局が証明書発行時に定めた有効期間の終了日時となり、証明書を失効しない限りこの日時まで証明書をご利用できます。</td></tr>
<tr><td>認証局</td><td>証明書を発行した認証局の世代を表示します。(G1 または G2 または G3)
<table>
<tr><th>名称</th><th>認証局世代</th><th>説明</th><th>署名アルゴリズム</th></tr>
<tr><td>G1</td><td>第 1 世代</td><td>2014 年 3 月 24 日以前に KDDI へ申請された証明書を管理している認証局</td><td rowspan="2">SHA-1</td></tr>
<tr><td>G2</td><td>第 2 世代</td><td rowspan="2">証明書カスタマーコントロール(本システム)から発行した証明書を管理している認証局</td></tr>
<tr><td>G3</td><td>第 3 世代</td><td>SHA-2(256)</td></tr>
</table></td></tr>
<tr><td>ポリシ ID</td><td>証明書発行時に指定した OS 種別や格納先、AuthID の情報が表示されます。</td></tr>
</table>

<table>
<tr><td>ステータス</td><td>証明書のステータスを表示します。

(主なステータス)
<table><tr><td>証明書発行(失効)申請中</td><td>認証局へ証明書の発行または失効の申請中。認証局の処理待ち。</td></tr><tr><td>証明書発行完了</td><td>認証局にて証明書の発行完了
(利用可能状態)</td></tr><tr><td>証明書の失効完了</td><td>認証局にて証明書の失効完了
(利用不可な状態)</td></tr><tr><td>有効期間終了</td><td>証明書の有効期間終了
(利用不可な状態)
ただし、時間差により本ステータスの値が『有効期間終了』でも、『有効期間の終了』の日時に至ってない場合は、証明書の利用可能</td></tr></table></td></tr>
<tr><td>署名アルゴリズム</td><td>証明書発行時に指定した値を表示します。(SHA-1/SHA-2(256))</td></tr>
<tr><td>鍵長</td><td>公開鍵の鍵長(2048bit)を表示します。</td></tr>
<tr><td>証明書発行申請日時</td><td>本カスタマーコントロールにて証明書発行申請を行った日時を表示</td></tr>
<tr><td>証明書の取得可否</td><td>端末側で証明書のインストールが可能か否かを表示します。
証明書のインストール期限を経過すると『不許可』となります。管理者さまによって『許可/不許可』を変更可能です。</td></tr>
<tr><td>証明書と秘密鍵の取得回数</td><td>利用端末が認証局に対して証明書を取得した回数を表示します。
本システムでの値の更新は 1 日 1 回(夜間)となります。
【再取得】ボタンにより認証局へ最新の値を取得しにいきます。</td></tr>
<tr><td>AuthID 種別</td><td>証明書発行時に指定した Auth ID の種類を表示します。
MAC アドレス/IMEI/UDID/GUID</td></tr>
<tr><td>AuthID</td><td>証明書発行時に指定した Auth ID の値を表示します。</td></tr>
<tr><td>UPN</td><td>証明書発行時に UPN(User Princpal Name)を指定した場合、その値が表示されます。</td></tr>
</table>

OS	証明書発行時に指定した OS 種別を表示します。
取得方法	Windows の場合、証明書発行時に指定した取得方法 (Importer/ActiveX)が表示されます。
証明書のメモ	証明書発行時に指定した『メモ』の値を表示します。 管理者さまによる変更可能な項目です。

6.2　証明書の取得可否変更

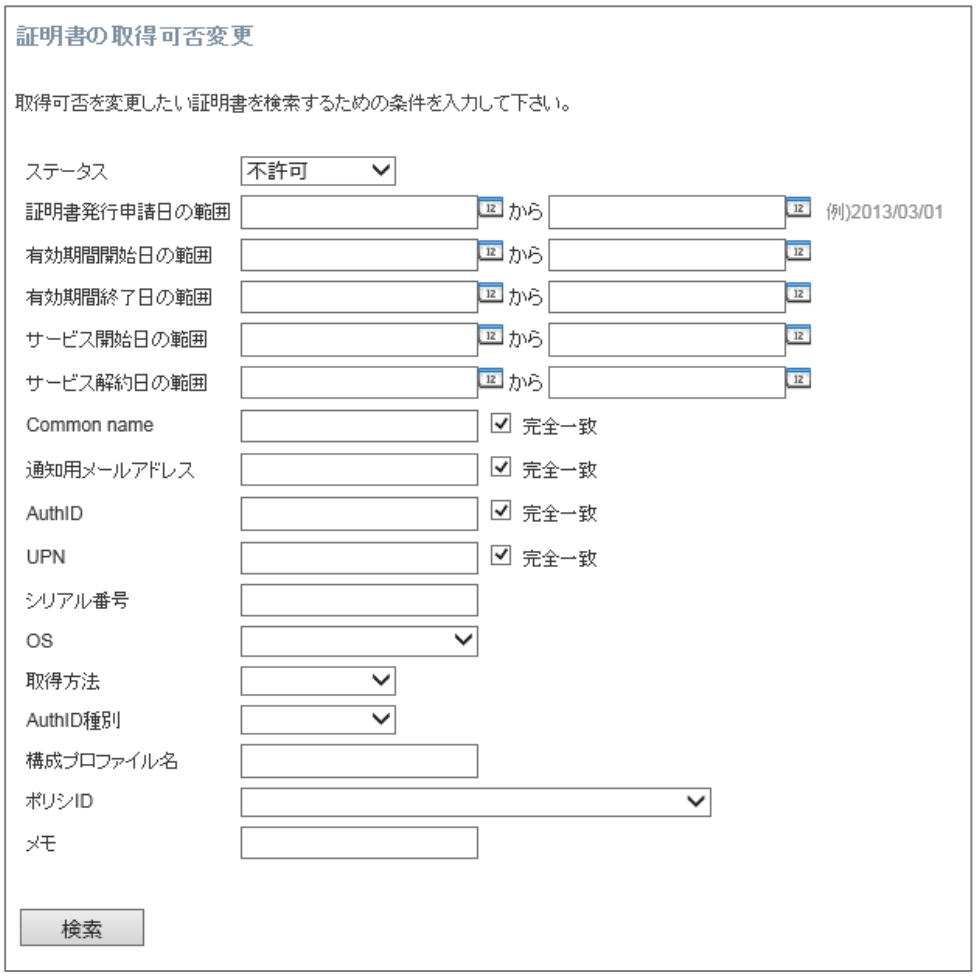
証明書は、発行から 1 週間経過した時点で取得(ダウンロード)ができなくなります。また一度取得された証明書は、取得後 3 日以内のみ再取得が可能となり取得可能期間が短縮されます。

本機能は、上記期限を経過後に再度取得を実施したい場合、また取得可能期間内においても手動で取得不可としたい場合に認証局側のステータスを変更することが可能です。

■ ステータスが許可の証明書を検索し選択・実行した場合、証明書取得ステータスを不許可へ変更します。

■ ステータスが不許可の証明書を検索し選択・実行した場合、証明書取得ステータスを許可へ変更します。(不許可→許可に変更した場合『再取得のお知らせ』メールが自動で送信されます)。

※ 証明書発行通知メールの再送信を申請したい場合、本操作にて行えます。



検索キーとしては以下の利用が可能です。

※ サービス開始日の範囲、サービス解約日の範囲はご利用になれません。

【検索キー】

検索キー	内容
ステータス	証明書申請後に検索可能なステータスは不許可/許可のみです。  ステータス情報と以降の検索項目の And 条件にて検索が実行されます。
証明書発行申請日の範囲	証明書発行処理をした日付を YYYY/MM/DD 形式で入力し検索可能です。日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間開始日の範囲	証明書有効期間開始日の範囲を YYYY/MM/DD 形式で入力し検索可能です。日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間終了日の範囲	証明書有効期間終了日の範囲を YYYY/MM/DD 形式で入力し検索可能です。日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
Common name	証明書に設定された CN 値検索が利用可能です。完全一致検索を行う場合はお客さまご利用 suffix 情報を含む、『xxxx@yyy』のメールアドレス形式にて検索してください。
通知用メールアドレス	発行通知メール送付先メールアドレスから検索可能です。
Auth ID	端末の MAC アドレス/IMEI/UDID の情報から検索可能です。 【注意】2014 年 3 月 24 日以前に KDDI に申請書を送付して発行された証明書情報の内 Windows®端末分については、Hash 処理された値で検索する必要があります。

UPN	証明書発行時に UPN を指定した場合 UPN の値で検索可能です。
シリアル番号	証明書のシリアル番号から検索可能です。
OS	OS 種別より検索可能です。
取得方法	取得方法より検索可能です。
AuthID 種別	MAC アドレス/IMEI/UDID/GUID の種別から検索可能です。
構成プロファイル名	iOS デバイスに適用している構成プロファイル名から検索が可能です。(部分一致) 【注意】構成プロファイル名は、ほかのお客さまとのユニーク性を確保するため証明書発行後は KDDI 指定ルールで保存されます。完全一致での検索を実施する場合証明書詳細情報を確認いただき OU 値に含まれる"Profile"から始まる値を入力ください。
ポリシ ID	OS 種別+AuthID 種別での複合検索キーとして利用可能です。以下プルダウンイメージから選択いただきます。  【注意】Android™用 AnyConnect 適用無は、KDDI に申請書を送付して発行された証明書の一部に適用されているポリシ ID です。本システムからの新規発行時にはご利用いただくことができません。
メモ	証明書発行時に記入したメモの値から検索が可能です。

検索結果が画面下部に表示されます。

表示された対象のシリアル番号列のチェックボックスにチェックを入れ、チェックデータのみ実行をクリックするか、検索条件に合ったすべての証明書に実行をクリックします。

本操作を実行することにより通知先メールアドレス設定に設定されたメールアドレスへ通知メールが送信されます。

【その他の方法で証明書の取得可否変更を実施する方法】

証明書の取得可否変更は、上記方法以外にも実施することが可能です。

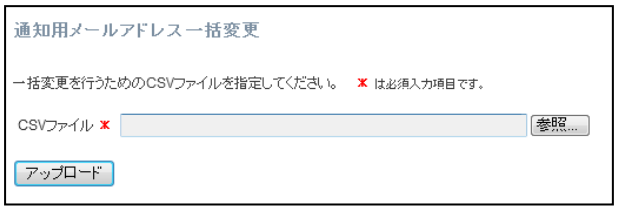
『12.2 証明書の詳細ステータス』ジョブ詳細画面にて、発行申請時に割り当てられた『リクエスト ID』『SubID』をクリックすると証明書ステータス変更画面が表示されます。または『6.1 申請情報の検索』検索結果表示後画面にて『シリアル番号』をクリックすると証明書ステータス変更画面が表示されます。証明書ステータス変更画面より取得可否設定を変更し、変更ボタンをクリックすることで証明書の取得可否変更が可能となります。

6.3　証明書のステータス更新

申請情報の検索画面より対象の証明書を選択し、申請情報の詳細画面の『再取得』ボタンをクリックすると、証明書の取得回数および取得可否のステータスの更新申請を行います。（認証局へ取得しに行くため時間を要します）

6.4　通知用アドレス一括変更

通知用アドレス一括変更では、CSV 形式フォーマットでファイルをアップロードすることにより通知用メールアドレスを一括変更します。



通知用メールアドレス一括変更の CSV ファイルフォーマットについては、『13.2 各種申請 CSV フォーマット』をご参照ください。

【その他の方法で証明書の通知先メールアドレス変更を実施する方法】

証明書の通知先メールアドレス変更は、上記方法以外にも実施することが可能です。

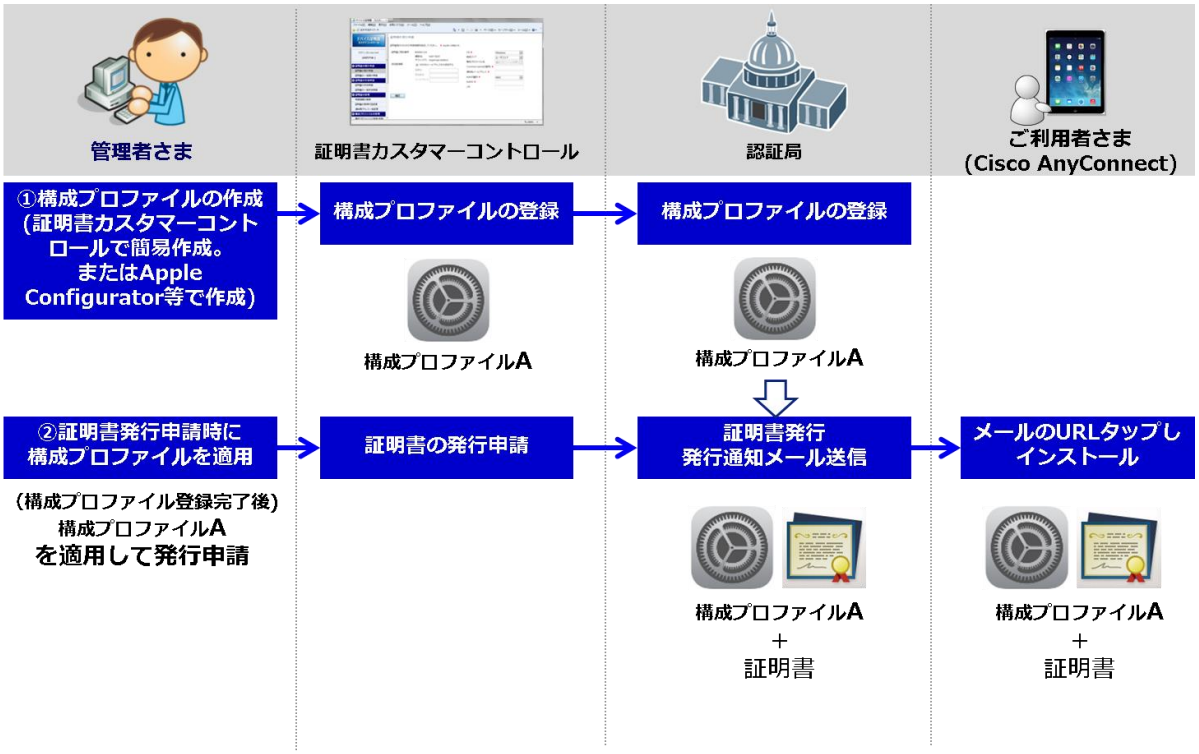
『12.2 証明書の詳細ステータス』ジョブ詳細画面にて、発行申請時に割り当てられた『リクエスト ID』『SubID』をクリックすると証明書ステータス変更画面が表示されます。または『6.1 申請情報の検索』検索結果表示後画面にて『シリアル番号』をクリックすると証明書ステータス変更画面が表示されます。証明書ステータス変更画面より通知先メールアドレス設定を変更し、変更ボタンをクリックすることで変更となります。

7 構成プロファイルの管理

本システムでは iOS デバイスに割り当てたい構成プロファイルを証明書と同時に配布し端末にインストールすることが可能です。

「KDDI FRE」のお客さまで iOS 版の『Cisco AnyConnect』を利用している場合は、事前に構成プロファイルを登録し、証明書発行時に登録した構成プロファイルを適用します。

例：構成プロファイルを適用した証明書をインストールするまでの流れ



7.1 構成プロファイルの作成方法

構成プロファイルの作成方法としては、以下のような方法があります。

認証方式	ケース・作成目的	作成方法
・Always-On 接続 **・ID＋証明書認証**	・『Cisco AnyConnect』を利用するためだけの設定をする場合(『Cisco Legacy AnyConnect』からの移行計画含む) ・iOS にて Always-On 接続を利用する場合 ・VPN のプロキシ設定のみできればよい場合	証明書カスタマーコントロールの『**構成プロファイルの簡易作成**』にて実施 **（自動作成）**
・オンデマンド接続 **・ID＋証明書認証**	・オンデマンド接続のドメインリストを設定する場合 ・『構成プロファイルの簡易作成』では設定項目が不足している場合	Apple Configurator にて作成 **（手動作成）**
すべて	・『Apple Configurator』では設定項目が不足している場合	その他ツールまたはテキストエディタなど **（手動作成）**

※ オンデマンド接続で対象のドメインリストを設定する際は、構成プロファイルにて設定してください。(『構成プロファイルの簡易作成』で登録した構成プロファイルをインストールした後、AnyConnect にてドメインリストの設定はできません。)

※ 「KDDI FRE」では、iOS 構成プロファイルの記述方法についてはサポート範囲外となります。Apple Configurator で作成する場合は、下記参考資料または Apple のヘルプ、ドキュメントなどをご参考にしてください。

※ テキストエディタで構成プロファイルを作成する際は、BOM(Byte Order Mark)が付与されない形式で保存ください。Windows®メモ帳の場合 BOM が付与され、構成プロファイルのアップロード時に認証局側で処理ができずエラーとなります。

◆『Cisco AnyConnect ver. 4.0.0707 以降』(新しい AnyConnect)を利用するための iOS 構成プロファイルの設定について

構成プロファイルの作成方法	『Cisco AnyConnect ver.40.0707 以降』を利用するための設定
証明書カスタマーコントロールの『**構成プロファイルの簡易作成**』にて作成する場合	選択項目「適用アプリ」にて、 ・AnyConnect ・(非推奨)AnyConnect & Legacy AnyConnect のどちらかを選択してください。
Apple Configurator にて作成する場合	『(参考資料) AnyConnect(iOS 版)に対応する iOS 構成プロファイル記述方法』を参考にして設定してください。
その他ツールまたはテキストエディタなど	**◆Cisco AnyConnect に対応** **<VPNSubType>キーにて** **com.cisco.anyconnect** を指定してください。 **◆Cisco Legacy AnyConnect に対応** **<VPNSubType>キーにて** **com.cisco.anyconnect.applevpn.plugin** を指定してください。

7.2 構成プロファイルの登録

作成した構成プロファイルを証明書カスタマーコントロールから認証局へ登録申請をします。登録申請は、証明書カスタマーコントロールの**『構成プロファイルの登録・削除』メニュー**から行えます。ただし、**『構成プロファイルの簡易作成』メニュー**では、システムが自動で作成から登録申請までを一貫して行います。

構成プロファイル (.mobileconfig)の作成	登録申請	本システム利用メニュー
Apple Configulator その他ツール	証明書カスタマー コントロール	構成プロファイルの登録・削除
証明書カスタマーコントロール		構成プロファイルの簡易作成

7.3 構成プロファイルの配布

構成プロファイルを登録した後、証明書発行申請時に『構成プロファイル』を指定して申請します。認証局から利用者へ証明書発行通知メールが送られ、メール内の URL をクリックすると該当の構成プロファイルと証明書が端末へインストールされます。

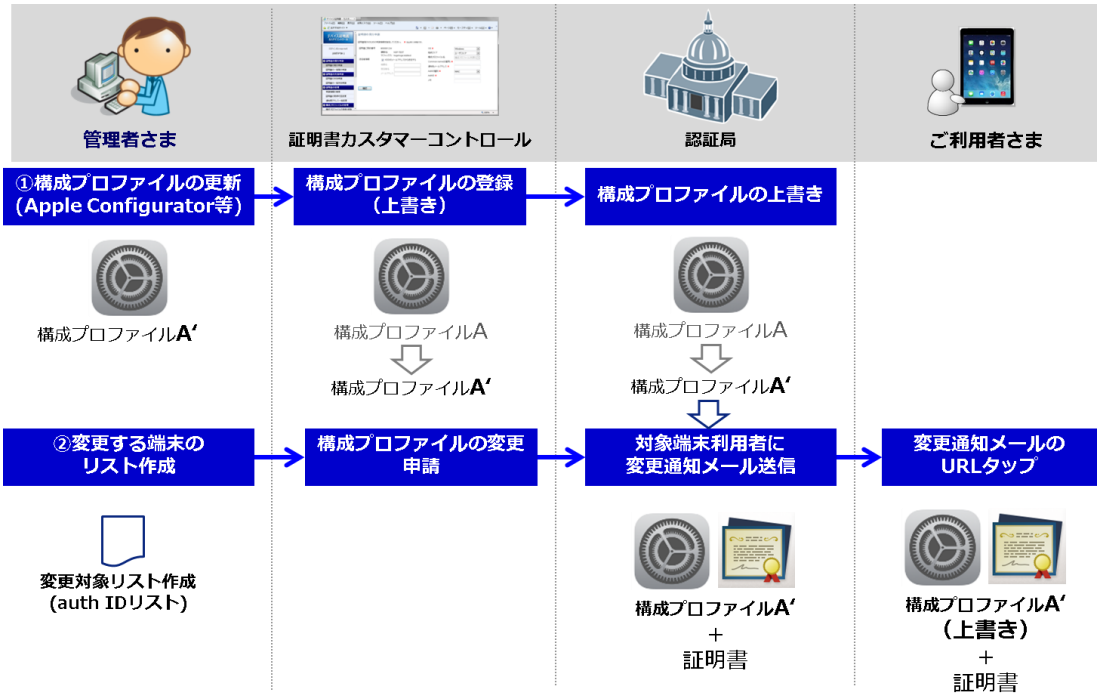
7.4 構成プロファイルの変更

既に端末にインストール済みの構成プロファイルについて変更を行う場合は、まず変更後の構成プロファイルを証明書カスタマーコントロールへ登録します。**『構成プロファイルの登録・削除』メニュー**で該当の構成プロファイルを『編集』するか、同一の構成プロファイル名でファイルを登録すると上書きされます。

その後、端末側への配布は**『構成プロファイルの変更』メニュー**で、対象端末を指定して申請します。認証局より利用者に変更通知のメールが送られ、メール内の URL をクリックすると新しい構成プロファイルをインストール(上書き)します。

◆構成プロファイル変更までの流れ(手動作成の場合)

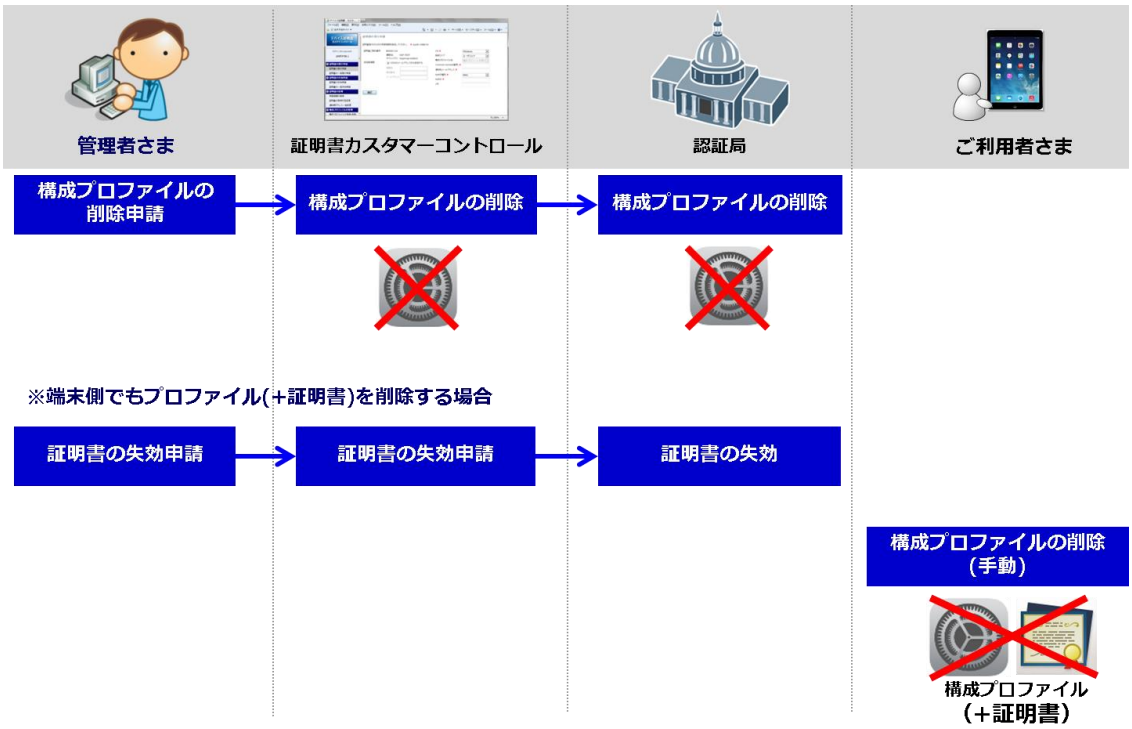
例: 構成プロファイル A を構成プロファイル A’ に更新する場合



※ 構成プロファイルの適用無しで発行した証明書について、後から構成プロファイルを適用したい場合は、新規に証明書を構成プロファイル適用して発行・インストールしていただき、古い証明書の失効と端末側での削除をしていただきます。(構成プロファイルの変更では行えません)

7.5 構成プロファイルの削除

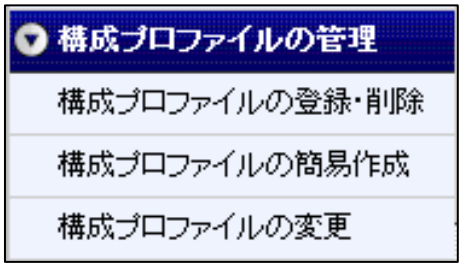
既に端末にインストール済みの構成プロファイル(と証明書)について削除を行う場合は、利用者さまが端末側で削除します。管理者さまは証明書カスタマーコントロールより認証局に対して登録済みの構成プロファイルの削除申請を行います。削除申請は**『構成プロファイルの登録・削除』メニュー**から行えます。



※ 端末側でもプロファイル(証明書)を削除する際には、証明書カスタマーコントロールにて該当の証明書の失効申請も行ってください。

7.6 証明書カスタマーコントロールのメニュー

メニュー領域より【構成プロファイルの管理】を選択すると以下のとおり管理メニューが表示されます。



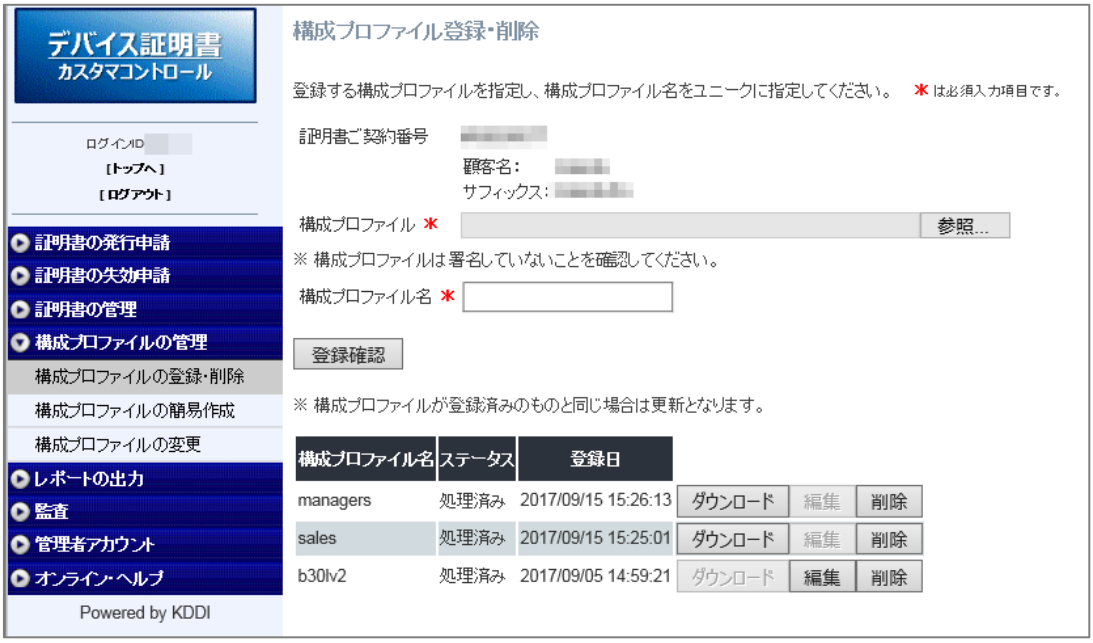
7.7 構成プロファイルの登録・削除

構成プロファイルの登録・削除では、iOS デバイスに割り当てたい構成プロファイルの登録・削除・編集が可能です。

構成プロファイルは、『Apple Configurator』などを用いて手動で作成いただくか、『7.8 構成プロファイルの簡易作成』メニューにて作成ください。

※『Cisco AnyConnect』を利用するための『Apple Configurator』の設定方法については、『(参考資料) AnyConnect(iOS 版)に対応する iOS 構成プロファイル記述方法』を参考にしてください。

※『Apple Configurator』の利用方法などの詳細については、ヘルプや Apple 社ウェブサイトなどをご確認ください。



【構成プロファイルを手動作成する場合】

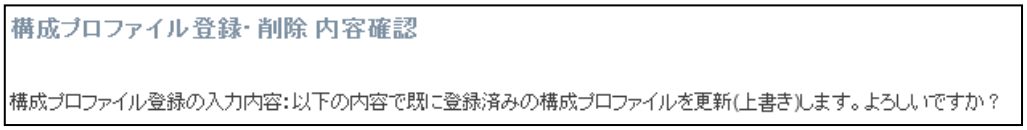
構成プロファイルを『Apple Configurator』にて作成いただくと『.mobileconfig』というファイルが生成されますので、該当ファイルを『参照』ボタンよりアップロードしてください。

【重要】構成プロファイルを iPhone 構成ユーティリティなどで作成する時に『エクスポート』をする際のセキュリティオプションは必ず『なし』を選択ください。

アップロードした構成ファイルに本システム内での管理用名称『構成プロファイル名』を付与し登録確認してください。なお、『構成プロファイル名』の文字数は、ご契約のサフィックス名の長さと合わせて合計 32 文字以内としてください。

過去に登録済の構成プロファイルをダウンロードしたい場合は、『ダウンロード』ボタンをクリックし該当ファイルをダウンロードすることが可能です。また内容削除する場合は、『削除』ボタンをクリックしてください。

【重要】構成プロファイルの内容の更新を実施する場合、過去に登録している『構成プロファイル名』と同じ名前を入力し新規登録同様の作業を実施することでファイルが上書きされます。その際に確認画面では、『既に登録済の構成プロファイルを更新(上書き)します』と表示されます。



※ 本システムへ構成プロファイル登録後、以下内容の認証局の形式チェックにより、処理 NG(注 1)となる可能性があります。構成プロファイル作成時にはご注意ください。

・XML 形式であること

・構成プロファイル名が半角であること(半角カタカナは NG)

・『PayloadIdentifier(注 2)』が存在すること

注 1)エラーメッセージの一例
『失敗したプロファイルが残されています。再度上書きしてください』
注 2)既存プロファイルの置き換えか、新たに追加するかを判断するためのプロファイル識別子。

【重要】「KDDI FRE」で『Always-On 接続』のご契約がないお客さまは、作成した構成プロファイルに常時接続動作となる項目が含まれている場合、アップロードができませんのでご留意ください。また、過去に登録している構成プロファイルも同ケースに該当する場合は、更新ができません。(注 3)

注 3)エラーメッセージの一例
『Always On ありの構成プロファイルはアップロードできません。W-DT1643』

【構成プロファイルの簡易作成メニューを利用する場合】
構成プロファイルの簡易作成メニューにて構成プロファイルを登録すると、本画面に構成プロファイル情報が追加されます。

登録済の構成プロファイルの内容変更をしたい場合は、『編集』ボタンをクリックし登録内容の修正が可能です。

※ 構成プロファイルの簡易編集画面が表示されます。（構成プロファイルの簡易作成画面と同一の画面です）

※ 簡易作成メニューにて登録した構成プロファイルをダウンロードすることはできません。

※ 簡易作成メニューで登録した構成プロファイルが『Cisco AnyConnect ver. 4.0.07077 以降』(iOS 版)に対応しているのは、2017 年 9 月 20 日以降に登録したものとなります。それ以前に作成した構成プロファイルを『Cisco AnyConnect ver. 4.0.07077 以降』(iOS 版)に対応させるためには、『編集』ボタンをクリックして再度『登録』を行って上書きしてください。

※ 2019 年 12 月 12 日より簡易作成メニューに「適用アプリ」項目が追加され、ご利用の AnyConnect アプリケーションに応じて「適用アプリ」を選択していただきます。ご利用の iOS および AnyConnect アプリケーションバージョンに適したプロファイルをご利用ください。AnyConnect アプリケーションと適用アプリの対応は以下をご参照ください。

※ *現在適用アプリに関して、(非推奨) AnyConnect & Legacy AnyConnect を選択いただいた場合でもサービスのご利用は可能ですが、今後 iOS 側で該当の構成プロファイルが読み込めなくなる可能性もあるため、最適な適用アプリを選択した上で簡易作成プロファイルをご利用いただくことを推奨します。*

『Cisco AnyConnect』での証明書の利用(構成プロファイル適用時)

簡易作成で登録した構成プロファイル		Cisco AnyConnect (ver. 4.0.07077～)	Cisco Legacy AnyConnet (ver. 4.0.05069)
	適用アプリ		
2019/12/12 以降に登録したもの(上書き含む)	AnyConnect	○ (利用可能)	× (利用不可)
	Legacy AnyConnect	× (利用不可)	○ (利用可能)
	(非推奨)AnyConnect & Legacy AnyConnect	○ (利用可能)	○ (利用可能)
2017/9/20～2019/12/11 に登録したもの(上書き含む)		○ (利用可能)	○ (利用可能)
2017/9/19 以前に登録したもの		× (利用不可)	○ (利用可能)

7.8 構成プロファイルの簡易作成

構成プロファイルの簡易作成では、iOS デバイスに割り当てたい構成プロファイルの簡易作成が可能です。

※ 本機能は「KDDI Flex Remote Access」契約者のみ利用可能です。

※ 構成プロファイルの一部項目のみの設定となります。

各項目で選択もしくは入力を行えます。必須項目を入力したのちに登録確認ボタンをクリックしてください。

入力項目が不正であった場合、登録確認ボタンをクリックするとエラーが表示されます。

項目		方式	内容
構成プロファイル名		入力	構成プロファイルの名称です。 お客さまのサフィックス名の文字数と合わせて、最大 39 文字以内
適用アプリ		選択	ご利用の AnyConnec アプリケーションに応じて適用アプリを ・AnyConnect ・Legacy AnyConnect ・(非推奨)AnyConnect&Legacy AnyConnect から選択します。
削除時のパスワード	（利用有無）	選択	iOS 端末にインストール後、構成プロファイルの削除時パスワード設定有無です。
	（文字列）	入力	構成プロファイル削除時に入力が必要となるパスワードの文字列です。
接続先 URL		KDDI 指定	「KDDI Flex Remote Access」サービス利用時に VPN 接続先 GW の URL 情報です。
Proxy サーバーの設定		選択	Proxy サーバーの設定を『自動/手動/なし』から選択します。
pac ファイルの URL		入力	Proxy サーバーの設定にて『自動』を選んだ場合のみ入力可能です。 pac ファイルの接続先 URL です。
Proxy サーバーのアドレス		入力	Proxy サーバーの設定にて『手動』を選んだ場合のみ入力可能です。 Proxy サーバーの IP アドレス、ポート番号、接続 ID、接続パスワードです。
Proxy サーバーのポート番号		入力	
Proxy サーバーへの接続 ID		入力	
Proxy サーバーへの接続パスワード		入力	
信頼できる NW（SSID で指定）		入力	

信頼できる NW（DNS ドメインで指定）	入力	「KDDI Flex Remote Access」の認証方式『Always-On 接続』契約者のみテキストボックスが表示され、入力可能です。 信頼できる NW 情報を SSID、または DNS ドメインで指定します。 ※ SSID と DNS ドメインの両方を指定することはできません。

※ 注意事項

・接続先 URL は、お客さま管理者アカウントの作成/変更時に KDDI 開通部門にて開通/切り替え日の前営業日迄（1～3 営業日前を目安）に登録します。

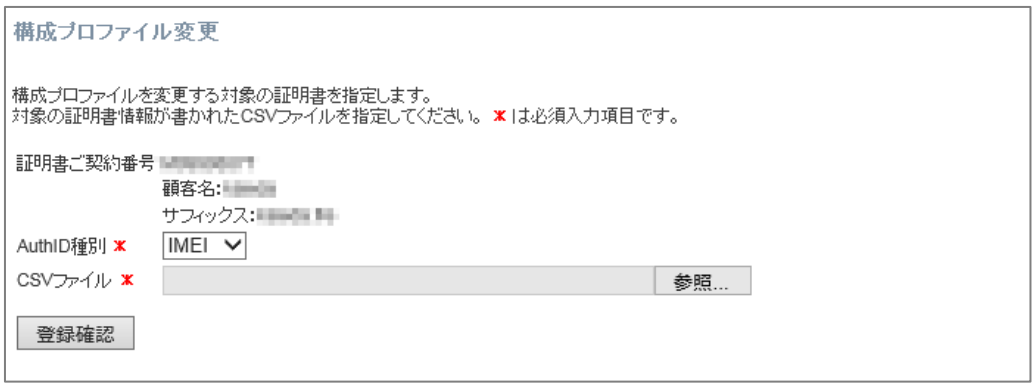
・接続先 URL の変更を伴う契約変更を行う場合、変更前の接続先 URL 情報を利用して構成プロファイルを作成することはできませんのでご注意ください。

・変更後の接続先 URL は、KDDI 法人営業担当者より送付される開通通知書をご確認ください。なお、『契約管理システム』をご利用の場合は、システム内の『契約内容照会』よりご確認できます。

・オンデマンド契約者は、本簡易作成機能で作成した構成プロファイルをご利用いただくことはできませんのでご注意ください。

7.9 構成プロファイルの変更

構成プロファイルの内容変更を実施した後に、各デバイスに対してアップデートを実施したい場合に本機能を利用します。



対象となる Auth ID 種別を選択し、申請情報の検索画面より構成プロファイル変更用 CSV をダウンロードし内容確認の上 CSV ファイルをアップロード、『登録確認』をクリックします。本操作実施により各デバイスの通知用メールアドレスに構成プロファイルの変更通知メールが送信されます。

※ 同一の Auth ID に対して、複数の証明書が発行されている場合、最新の発行済証明書の通知用メールアドレスに対してのみ変更通知メールが 1 通送信されます。

8 レポートの出力

レポートの出力では、過去 6 カ月分の証明書利用状況を出力可能です。

8.1 証明書のレポート

証明書のレポートでは、過去 6 カ月(月初-月末締め)分もしくは最新の有効証明書の情報検索が可能です。

【レポートの種類】

レポートの種類	内容
有効証明書	発行済で失効されていない証明書 ※ 課金対象の証明書
発行済み証明書	正常に発行処理された証明書
失効済み証明書	正常に失効処理された証明書
未取得証明書	発効後、端末側で取得されていない証明書
取得済証明書	発効後、端末側で取得された証明書 【注意】稀に端末側へダウンロードされたがインストールに失敗したケースや、途中で利用者がインストール処理を中断してインストールが完了していないケース

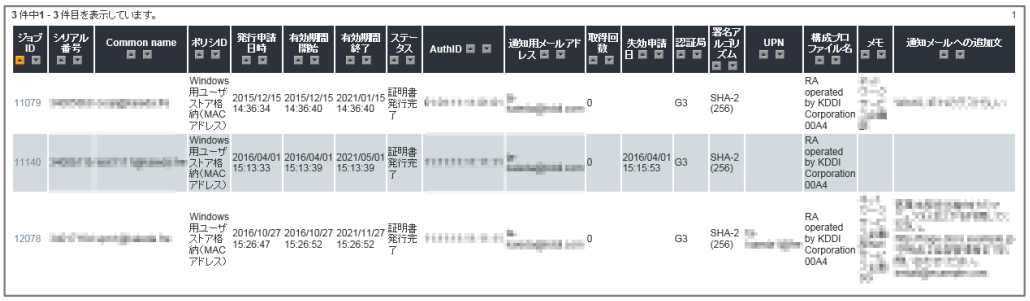
	がありますが、ダウンロードされた時点で『取得済』とカウントされます）

検索キーとしては以下の利用が可能です。

検索キー	内容
ご利用月	最新もしくは過去 6 カ月分の中から対象を選択します。
レポートの種類	有効な証明書
Common name	証明書に設定された CN 値検索が利用可能です。完全一致検索を行う場合はお客さまご利用 suffix 情報を含む、『xxxx@yyy』のメールアドレス形式にて検索してください。
ポリシ ID	OS 種別+AuthID 種別での複合検索キーとして利用可能です。 以下プルダウンイメージから選択いただきます。 Windows用コンピュータストア格納（MACアドレス） Windows用ユーザストア格納（MACアドレス） Windows Mobile用（GUID） iPhone/iPad用（IMEI） iPhone/iPad用（UDID） Android用AnyConnect適用有（IMEI） Android用AnyConnect適用有（MACアドレス） Android用AnyConnect適用無（IMEI） Android用AnyConnect適用無（MACアドレス） MAC OS用（MACアドレス） 【注意】Android™用 AnyConnect 適用無は、KDDI に申請書を送付して発行された証明書の一部に適用されているポリシ ID

	です。本システムからの新規発行時にはご利用いただくことができません。
証明書発行申請日の範囲	証明書発行処理をした日付を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間開始日の範囲	証明書有効期間開始日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。
有効期間終了日の範囲	証明書有効期間終了日の範囲を YYYY/MM/DD 形式で入力し検索可能です。 日付範囲での検索も可能です。カレンダーマークをクリックすることで日付を選択することも可能となります。

検索ボタンをクリックすると、検索結果が画面下部に表示されます。



※ 注意事項

『メモ』または『通知メールへの追加文』の長さによって、行の幅が大きくなることがございます。画面下部の検索結果に見えない場合は画面をスクロールしてご確認ください。

検索結果の項目は以下のとおりです。

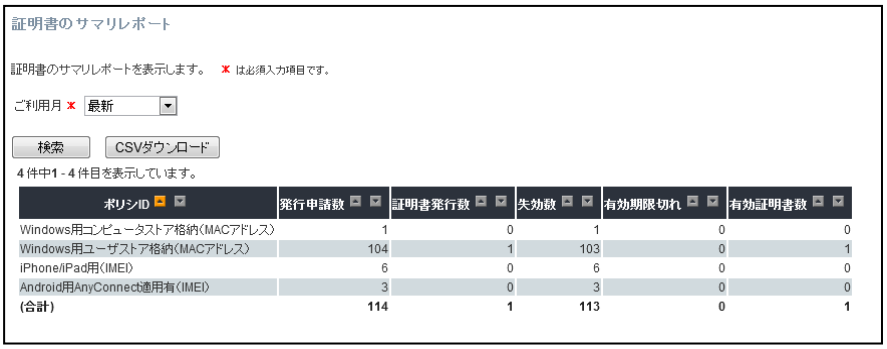
項目名	内容
ジョブ ID	申請ごとに割り当てられる ID です。
シリアル番号	証明書ごとに固有なキーであるシリアル番号が表示されます。

<table>
<tr><td>Common name</td><td>証明書の Common Name が表示されます。</td></tr>
<tr><td>ポリシ ID</td><td>OS 種別+AuthID 種別となります。以下プルダウンイメージの値のいずれかになります。
 
</td></tr>
<tr><td>発行申請日時</td><td>証明書発行申請された日時が表示されます。</td></tr>
<tr><td>有効期間開始</td><td>有効期間開始日時が表示されます。</td></tr>
<tr><td>有効期間終了</td><td>有効期間終了日時が表示されます。</td></tr>
<tr><td>ステータス</td><td>証明書の最終ステータスが表示されます。</td></tr>
<tr><td>AuthID</td><td>端末の MAC アドレス/IMEI/UDID の情報です。</td></tr>
<tr><td>通知用メールアドレス</td><td>発行通知メール送付先メールアドレスが表示されます。</td></tr>
<tr><td>取得回数</td><td>端末側で証明書を取得された回数が表示されます。</td></tr>
<tr><td>失効申請日</td><td>証明書失効申請された日時が表示されます。</td></tr>
<tr><td>認証局</td><td>認証局の世代を表します。
<table>
<tr><th>名称</th><th>認証局世代</th><th>説明</th><th>署名アルゴリズム</th></tr>
<tr><td>G1</td><td>第 1 世代</td><td>2014 年 3 月 24 日以前に KDDI へ申請された証明書を管理している認証局</td><td rowspan="2">SHA-1</td></tr>
<tr><td>G2</td><td>第 2 世代</td><td rowspan="2">証明書カスタマーコントロール(本システム)から発行した証明書を管理している認証局</td></tr>
<tr><td>G3</td><td>第 3 世代</td><td>SHA-2(256)</td></tr>
</table></td></tr>
</table>

署名アルゴリズム	デジタル署名に用いるアルゴリズム(ハッシュ関数の種類)を表します。
UPN	証明書発行時に UPN を指定した場合 UPN の値が表示されます。
構成プロファイル名	iOS デバイスに適用している構成プロファイル名が表示されます。
メモ	証明書発行時に記入したメモの値が表示されます。
通知メールへの追加文	証明書発行時に記入した通知メールへの追加文の値が表示されます。
適用アプリ	iOS デバイスに適用している構成プロファイルの適用アプリが表示されます(構成プロファイルの簡易作成で作成したプロファイルを利用している場合のみ)。

8.2 証明書のサマリレポート

証明書のサマリレポートでは、過去 6 カ月(月初-月末締め)分もしくは最新の発行済、失効済などのサマリ情報を確認することができます。表示情報を CSV としてダウンロードすることが可能です。



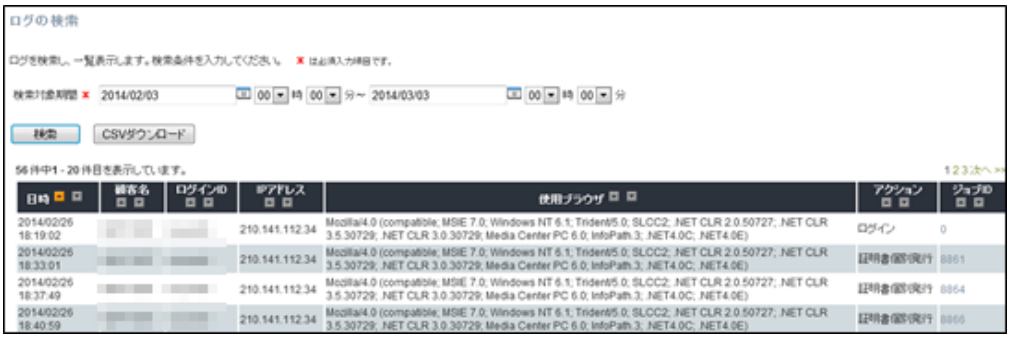
9 監査

監査では、管理者さまが実施された操作ログの閲覧が可能です。

9.1 ログの検索

過去 6 カ月以内の検索対象期間を指定し、管理者さまが操作されたログの閲覧が可能です。

『CSV ダウンロード』ボタンをクリックすることで該当データをダウンロードすることが可能です。 ダウンロードファイル名は、『監査ログ_″yyyymmddhhmm″.csv』となります。

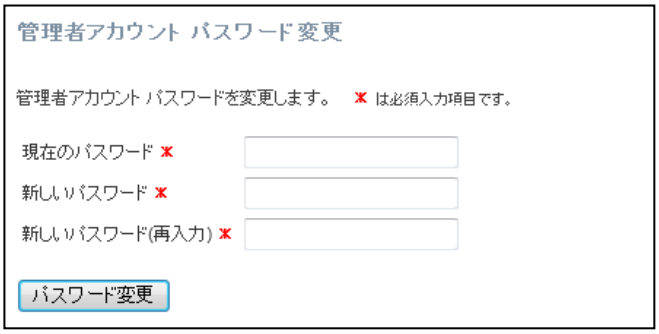


10 管理者アカウント

管理者アカウントでは、管理者さまによるログインパスワード変更が可能です。

10.1 パスワードの変更

現在のパスワードおよび新しいパスワードを 2 回(確認用含)入れて『パスワード変更』をクリックすることでパスワードが変更されます。



管理者アカウントのログインパスワードの文字制限事項は、以下のとおりです。

・半角英数文字(記号は利用不可)8 文字以上、16 文字以内

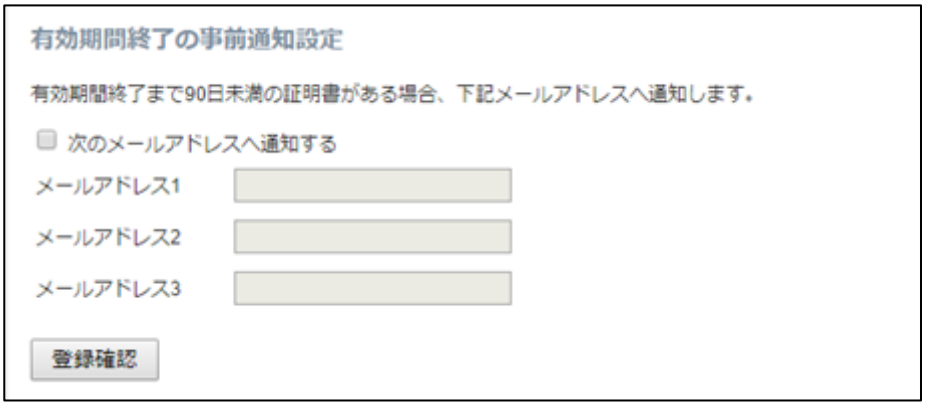
・英字と数字の混在必須

・ログイン ID と同値、現在のパスワードと同値は利用不可

10.2 有効期間終了通知設定

直近 3 カ月にて有効期間(5 年 1 カ月)が満了となる証明書の枚数を事前に登録されたメールアドレス宛へ月初に通知します。

※ 最大 3 つまで通知先メールアドレスの登録が可能です。
※ 既に登録済みの場合は、登録されたメールアドレスが表示されます。
※「次のメールアドレスへ通知する」にチェックを入れて、事前通知設定を
　登録すると通知機能が有効に、はずして登録すると通知機能が無効になります。
※ 登録後、通知先メールアドレスにテストメールが送信されます。



登録ボタンを押下し事前通知設定を登録します。

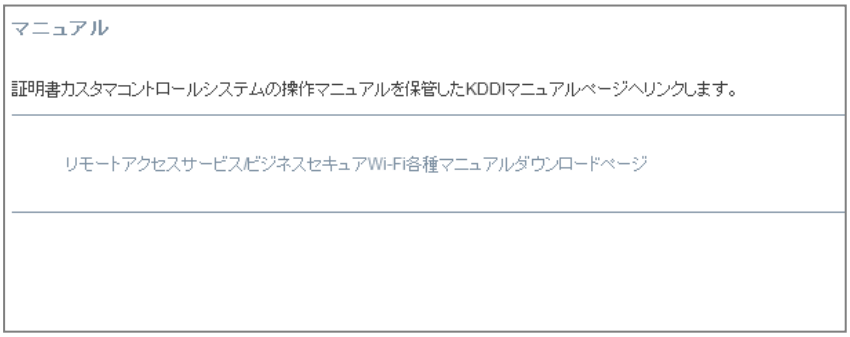
通知されるメールフォーマットについては、『13.1 メールフォーマット』をご参照ください。

11 オンライン・ヘルプ

オンライン・ヘルプでは、マニュアル掲載ページへのリンク、お知らせ内容を確認することができます。

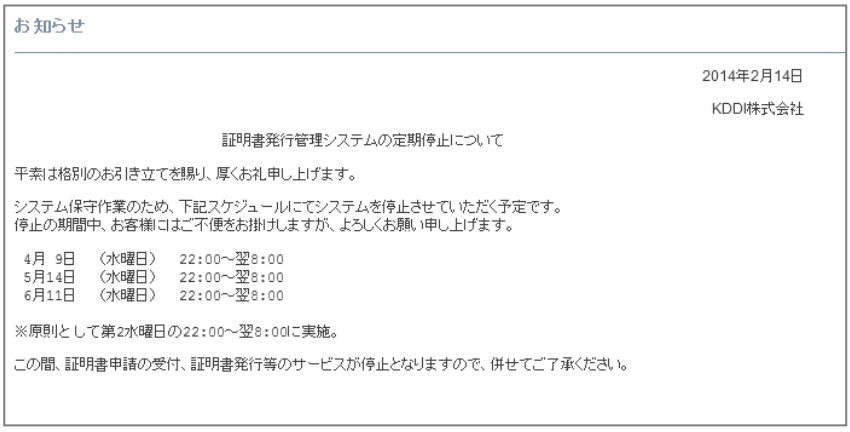
11.1 マニュアル

マニュアルは、本資料や KDDI 各リモートアクセスサービスの『RADIUS カスタマーコントロール』を含むマニュアル掲載ページへのリンクが表示されます。



11.2 お知らせ

本ページにおいて、システムメンテナンスによる停止日時などのお知らせ情報をご連絡します。



※ 本ページは、イメージです。

12 各種処理状況の確認

認証局への各種申請を実施することで『ジョブ ID』が発行されます。

過去 6 カ月間に発行されたジョブは、ログイン後トップ画面よりステータス(処理状況)を確認いただくことが可能です。

※ 初期状態では、完了となった処理は表示されません。完了後の状況確認が必要な場合は、画面上チェックボックスをオンにしてください。

※ 画面左上の以下画像リンクをクリックすることで、ジョブのステータス(処理状況)が表示されます。

※ 処理状況の画面イメージは以下のとおりです。

12.1 各処理のステータス

認証局への処理は、進行状況があります。

各処理申請の進行状況は以下のとおりです。

ジョブのステータス	内容
申請処理待ち	登録された処理(ジョブ)が、プログラムに検出されるまでの状態です。

申請処理中	登録された処理(ジョブ)が、プログラムに検出され必要なファイルの生成などを実施している状態です。
CA 処理中	登録された処理(ジョブ)により生成されたファイルが認証局に送付され処理が行われている状態です。
申請処理完了	登録された処理(ジョブ)により生成されたファイルが認証局に送付され処理が行われ正常に処理が完了した状態です。
申請処理 NG	登録された処理(ジョブ)により生成されたファイルが認証局に送付され処理が行われたが、タイムアウトの発生などにより処理が正常終了しなかった状態です。

12.2 証明書の詳細ステータス

上記ジョブのステータス内でさらに詳細なステータス情報があります。

『ジョブ ID』をクリックして詳細確認することができます。

※『リクエスト ID』『SubID』をクリックすることで証明書申請情報の詳細画面へ進みます。

表示項目	内容
リクエスト ID	証明書発行申請を管理するための認証局側のユニークな数値となります。

SubID	証明書発行処理中に証明書発行完了までの証明書管理用 ID となります。
アクション	発行、失効などの処理の種別が表示されます。
ログイン ID	上記アクションの処理をしている ID を表示します。 ※ システム内 ID が処理している項目も表示されます。
ステータス	ジョブのステータスを表示します。
タイムスタンプ	ステータスが登録(変更)された日時を表示します。
備考	証明書発行時に登録されたメモを表示します。

ステータス詳細は以下のとおりです。

詳細ステータス	内容
証明書発行申請処理待ち	発行申請処理がプログラムに検出されるまでの状態です。
証明書失効申請処理待ち	失効申請処理がプログラムに検出されるまでの状態です。
証明書取得可否変更申請処理待ち	取得可否変更申請がプログラムに検出されるまでの状態です。
通知用アドレス一括変更申請処理待ち	通知用アドレス一括変更申請処理がプログラムに検出されるまでの状態です。
申請情報取得申請処理待ち	発行申請処理など証明書が発行された後の状態(情報)を取得する処理がプログラムに検出されるまでの状態です。
構成プロファイル変更申請処理待ち	構成プロファイル変更申請処理がプログラムに検出されるまでの状態です。
証明書発行申請処理中	発行申請処理がプログラムに検出され必要なファイルの生成などを実施している状態です。

証明書失効申請処理中	失処申請処理がプログラムに検出され必要なファイルの生成などを実施している状態です。
証明書取得可否変更申請処理中	取得可否変更申請がプログラムに検出され必要なファイルの生成などを実施している状態です。
通知用アドレス一括変更申請処理中	通知用アドレス一括変更申請処理がプログラムに検出され必要なファイルの生成などを実施している状態です。
構成プロファイル変更申請処理中	構成プロファイル変更申請処理がプログラムに検出され必要なファイルの生成などを実施している状態です。
証明書発行完了	発行申請処理により証明書の発行が認証局で完了した状態です。
証明書の失効完了	失効申請処理により証明書の失効が認証局で完了した状態です。
証明書取得可否変更申請処理中	取得可否変更申請処理により証明書の取得可否変更が認証局で完了した状態です。
通知用アドレス一括変更申請処理完了	通知用アドレス一括変更申請処理により証明書の取得可否変更が認証局で完了した状態です。
構成プロファイル変更申請処理完了	構成プロファイル変更申請処理により証明書の取得可否変更が認証局で完了した状態です。
証明書取得可否変更申請処理中	取得可否変更申請がプログラムに検出され必要なファイルの生成などを実施している状態です。
申請処理 NG	各申請処理がタイムアウトなどにより NG となった場合に表示されます。

13 各種フォーマット(メールフォーマット/各種申請 CSV フォーマット)

13.1 メールフォーマット

【発行通知メールサンプル(iOS デバイスの例)】

差出人	no-reply@deviceid.kddi.ne.jp （または、お客さま指定の『メールアドレス』） ①
宛先	証明書発行申請時の『通知先メールアドレス』
件名	サイバートラスト デバイス ID 発行のお知らせ

②

KDDI 株式会社（またはお客さま指定の『組織名』）の申請により、デバイス ID が
発行されました。
以下の手順に従い、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。

※下記の手順で、ブラウザは Safari をお使いください。

手順 1:
iPhone または iPad で以下の URL にアクセスしてデバイス ID 認証局証明書をインストールしてください。
「プロファイルがダウンロードされました」のダイアログが表示された場合には、インストールが完了しておりませんので、以下の操作を行ってください。
[設定] - [一般] - [プロファイル]から、ダウンロード済みプロファイルのインストール操作を続行してください。
※パスコードを設定している場合、途中でパスコード入力を求められます。
※デバイス ID 認証局証明書のインストール完了後、このメールに戻り、手順 2 に進んでください。
https://www.cybertrust.ne.jp/deviceid/g2.crt

手順 2:
iPhone または iPad で以下の URL にアクセスしてデバイス ID をインストールしてください。
「プロファイルがダウンロードされました」のダイアログが表示された場合には、インストールが完了しておりませんので、以下の操作を行ってください。
[設定] - [一般] - [プロファイル]から、ダウンロード済みプロファイルのインストール操作を続行してください。
※パスコードを設定している場合、途中でパスコード入力を求められます。
https://cybertrust.deviceid.ne.jp/iPhoneOTA/do/start?sd=DiDk&reqID=XXXXXXXXXXXXXXX

※プロファイルのインストールに失敗した場合（プロファイルの削除を求められた場合）、以下の URL をお試しください。
https://cybertrust.deviceid.ne.jp/iPhoneOTA/do/start?sd=DiDk&reqID=XXXXXXXXXXXXXXX

デバイス ID 情報
リクエスト ID　: 201XXXXXXXXX
コモンネーム　: XXXXXX@XXXXXXXXX
シリアル番号　: XXXXXXXX
証明書有効期間: 2016/XX/XX-22:37:48 - 2021/XX/XX-22:37:48

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。

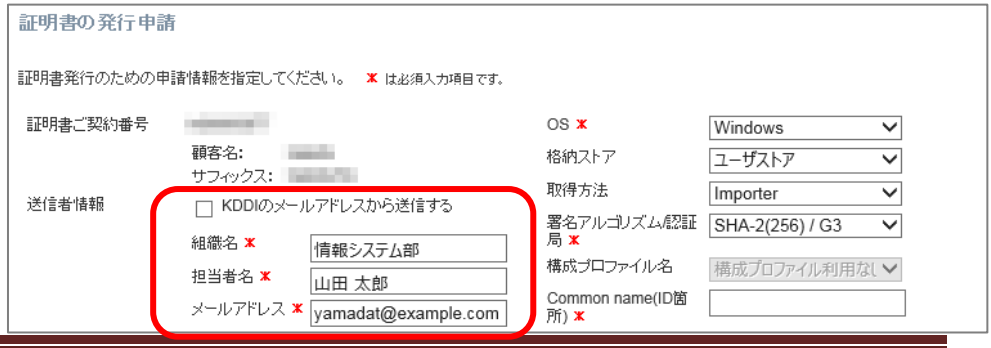
<<通知メールへの追加文>>xxxxxxxxxxxxx

KDDI 株式会社（またはお客さま指定の『組織名』）
証明書発行担当（またはお客さま指定の『担当者名』）　③

【解説】

証明書発行申請時の『送信者情報』の設定により差出人および本文の一部を変更できます。

変更可能な箇所	送信者情報(発行申請時)	
	『KDDI のメールアドレスから送信する』にチェックした場合	『KDDI のメールアドレスから送信する』にチェックしない場合
①差出人	no-reply@deviceid.kddi.ne.jp	お客さま指定のメールアドレス
②1 行目	KDDI 株式会社の申請により・・	お客さま指定の組織名により・・
③フッター	KDDI 株式会社 証明書発行担当	お客さま指定の組織名 お客さま指定の担当者名



【発行通知メールサンプル(Android™デバイスの例)】

差出人	no-reply@deviceid.kddi.ne.jp （または、お客さま指定の『メールアドレス』）
宛先	証明書発行申請時の『通知先メールアドレス』 ②
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（またはお客さま指定の『組織名』）の申請により、デバイス ID が発行されました。
以下の手順に従い、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。

手順 1:
Android で以下の URL にアクセスして Android 専用デバイス ID アプリケーションをインストールしてください。
※URL をタップした後、「アプリを選択」ダイアログで「Play ストア」または「マーケット」を選択してください。
※無線 LAN 経由でアクセスした場合はインストールできないことがありますので、3G 回線でアクセスしてください。
※最新のバージョンでのみ動作が保証されます。すでに Android 専用デバイス ID アプリケーションをインストール済みの場合でも、URL をタップし最新のバージョンをインストールしてください。
http://market.android.com/details?id=jp.ne.cybertrust.deviceid

手順 2:
Android で以下の URL にアクセスして AnyConnect をインストールしてください。
※URL をタップした後、「アプリを選択」ダイアログで「Play ストア」または「マーケット」を選択してください。
※インストール完了後に AnyConnect を起動してください。
※AnyConnect が英語の同意確認画面を表示します。利用規約をご確認の上、承認してください。
※オプションメニューから"設定" > "外部制御" > "プロンプト"の順にタップしてください。
https://market.android.com/details?id=com.cisco.anyconnect.vpn.android.avf

手順 3:
Android で以下の URL にアクセスしてデバイス ID を AnyConnect にインストールしてください。
※URL にアクセスすると、Android 専用デバイス ID アプリケーションが起動します。
※Android 専用デバイス ID アプリケーションにて、利用規約を確認後、「同意する」ボタンをタップしてください。
※パスワードを任意の 6 から 12 文字の数字で入力し、「証明書の取得」ボタンをタップしてください。
※パスワードの入力を求められますので、入力画面で指定したパスワードを入力してください。
https://cybertrust.deviceid.ne.jp/ee/androidAppLauncher.jsp/sd=DiDk&cd=G3k&pd=DeviceiD_KDDI_Android_IMEI_Cisco&rd=201711210242416&rfd=gYnW8oOa&cst=1

手順 4:
Android で以下の URL にアクセスして AnyConnect のネットワーク設定をしてください。
※AnyConnect の起動を求められますので、「OK」をタップしてください。
※ネットワーク設定の作成が成功した場合 Successfully…から始まるダイアログが表示されますので、「OK」をタップしてください。

https://cybertrust.deviceid.ne.jp/ee/anyConnectVpn.jsp/an=&ah=&ac=and%40cybertrust

手順 5:
無線 LAN や Web のアクセスで機器認証を利用する場合、Android で以下の URL にアクセスしてデバイス ID をインストールしてください。
※URL にアクセスすると、Android 専用デバイス ID アプリケーションが起動します。
※Android 専用デバイス ID アプリケーションにて、利用規約を確認後、「同意する」ボタンをタップしてください。
※パスワードを任意の 6 から 12 文字の数字で入力し、「証明書の取得」ボタンをタップしてください。
※パスワードの入力を求められますので、入力画面で指定したパスワードを入力してください。
※証明書の名前の入力を求められますので、任意の名前を入力してください。
※画面ロック方法によっては、証明書インストール時に認証情報ストレージパスワード入力を求められることがあります。
※Android 4.3 以降をご利用の場合、証明書インストール時に認証情報の使用に関する選択肢が表示されます。
証明書の用途に合わせて「VPN とアプリ」もしくは、「Wi-Fi」を選択してください。
https://cybertrust.deviceid.ne.jp/ee/androidAppLauncher.jsp/sd=DiDk&cd=GXX&pd=DeviceiD_KDDI_Android_IMEI_Cisco&rd=2017XXXXXXXX16&rfd=XXXXXXXXX

デバイス ID 情報
リクエスト ID　: 2017XXXXXXXXX
コモンネーム　: (idname)@(suffixname)
シリアル番号　: 34XXXXXX
証明書有効期間: 2017/XX/XX-XX:XX:XX - 2022/XX/XX-XX:XX:XX

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。

<<通知メールへの追加文>>xxxxxxxxxxxxx

KDDI 株式会社（またはお客さま指定の『組織名』）
証明書発行担当（またはお客さま指定の『担当者名』）
---

③

【取得可否変更メールサンプル(iOS デバイスの場合)】

差出人	no-reply@deviceid.kddi.ne.jp （または、お客さま指定の『メールアドレス』）
宛先	証明書に設定されている『通知先メールアドレス』
件名	サイバートラスト デバイス ID 再取得のお知らせ

KDDI 株式会社（またはお客さま指定の『組織名』）の申請により、デバイス ID の再取得が可能になりました。
以下の手順に従い、デバイス ID をインストールしてください。

デバイス ID は本メールの送信から 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。
本メールの送信から 7 日を経過した場合は、管理者へお問い合わせください。
※下記の手順で、ブラウザは Safari をお使いください。

手順 1:
iPhone または iPad で以下の URL にアクセスしてデバイス ID 認証局証明書をインストールしてください。
※パスコードを設定している場合、途中でパスコード入力を求められます。
※デバイス ID 認証局証明書のインストール完了後、このメールに戻り、手順 2 に進んでください。
https://www.cybertrust.ne.jp/deviceid/g2.crt

手順 2:
iPhone または iPad で以下の URL にアクセスしてデバイス ID をインストールしてください。
※パスコードを設定している場合、途中でパスコード入力を求められます。
※iOS 4.0 未満の場合、デバイス ID をインストールする際に別途パスワード入力を求められますので、下記のパスワードを入力してください。
パスワード: cybertrust
https://cybertrust.deviceid.ne.jp/iPhoneOTA/do/start?sd=DiDk&reqID=XXXXXXXXXXXXXX

※プロファイルのインストールに失敗した場合（プロファイルの削除を求められた場合）、以下の URL をお試しください。
https://cybertrust.deviceid.ne.jp/iPhoneOTA/do/start?sd=DiDk&reqID=XXXXXXXXXXXXXX

デバイス ID 情報
リクエスト ID : 201XXXXXXXXXXXX
コモンネーム : XXXXX@XXXXXXXX
シリアル番号 : XXXXXXXX
証明書有効期間: 2016/XX/XX-22:37:48 - 2021/XX/XX-22:37:48

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（またはお客さま指定の『組織名』）
証明書発行担当（またはお客さま指定の『担当者名』）

【構成プロファイル変更通知メールサンプル】

差出人	no-reply@deviceid.kddi.ne.jp（または、お客さま指定の『メールアドレス』）
宛先	証明書に設定されている『通知先メールアドレス』
件名	サイバートラスト デバイス ID 構成プロファイル変更のお知らせ

KDDI 株式会社（またはお客さま指定の『組織名』）の申請により、構成プロファイルが変更されました。
以下の手順に従い、デバイス ID をインストールしてください。

デバイス ID は本メールの送信から 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。
本メールの送信から 7 日を経過した場合は、管理者へお問い合わせください。

手順:
iPhone または iPad で以下の URL にアクセスしてデバイス ID をインストールしてください。
※パスコードを設定している場合、途中でパスコード入力を求められます。
※iOS 4.0 未満の場合、デバイス ID をインストールする際に別途パスワード入力を求められますので下記のパスワードを入力してください。
パスワード:cybertrust
https://cybertrust.deviceid.ne.jp/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

デバイス ID 情報
リクエスト ID:XXXXXXXXXXXXXX
コモンネーム:XXXXX@XXXXXXXX
シリアル番号:XXXXXXXXXX
証明書有効期間:2014/03/03-14:22:44 - 2019/04/03-14:22:44

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（またはお客さま指定の『組織名』）
証明書発行担当（またはお客さま指定の『担当者名』）

【有効期間終了の事前通知メールサンプル】

差出人	no-reply@deviceid.kddi.ne.jp
宛先	事前通知設定に登録されている『通知先メールアドレス』
件名	【KDDI】証明書(一部)の有効期間満了のお知らせ

KDDI FRE/ビジネスセキュア Wi-Fi
証明書認証ご利用者さま

直近 3 カ月にて有効期間(5 年 1 カ月)が満了となる
証明書がございますのでご確認ください。

■有効期間満了の予定 (YYYY 年 MM 月 DD 日 hh:mm 抽出時点)

証明書契約 M 番号:Mxxxxxxxx
YYYY 年 MM 月中満了分:x,xxx 枚
YYYY 年 MM 月中満了分:x,xxx 枚
YYYY 年 MM 月中満了分:x,xxx 枚

対象証明書の詳細につきましては証明書カスタマーコントロールよりご確認ください。
※ 抽出からメール受信までの間にお客さま操作があった場合は、対象枚数に相違がある場合がございます。

有効期間が満了した証明書は本サービスのご利用は出来なくなります。
継続してご利用の場合は証明書カスタマーコントロールより、新規に証明書を発行して端末にインストールしてください。
※有効期間が満了した証明書は自動的に課金対象外となります。

・証明書カスタマーコントロール URL
https://ccs01.deviceid.kddi.ne.jp/deviceid_admin

※ 詳細の利用方法につきましては以下マニュアルをご参照ください。
http://media3.kddi.com/extlib/files/business/download/pdf/certificate-manual.pdf
- 2.1 章:証明書発行申請の方法
- 8.1 章:証明書の有効期間確認方法

本メールは送信専用のメールアドレスから送信されております。
このままご返信いただいてもお答えできませんのでご了承ください。
なお、証明書カスタマーコントロールの操作方法については、
法人お客さまセンターまでお問い合わせください。

＜お問い合わせ先＞
法人お客さまセンター
電話:0077-7007(0120-921-919)
受付時間:9:00～18:00 ※土・日・祝日・年末年始を除く
KDDI 株式会社

【有効期間終了の通知先設定アドレスへのテストメールサンプル】

差出人	no-reply@deviceid.kddi.ne.jp
宛先	事前通知設定に登録されている『通知先メールアドレス』
件名	【KDDI】宛先メールアドレス登録完了のお知らせ

KDDI FRE/ビジネスセキュア Wi-Fi
証明書認証ご利用者さま

証明書カスタマーコントロールにて、証明書有効期間満了通知の
宛先メールアドレスの登録が完了しましたのでお知らせします。

・証明書カスタマーコントロール URL
https://ccs01.deviceid.kddi.ne.jp/

本メールは送信専用のメールアドレスから送信されております。
このままご返信いただいてもお答えできませんのでご了承ください。

KDDI 株式会社

13.2 各種申請 CSV フォーマット

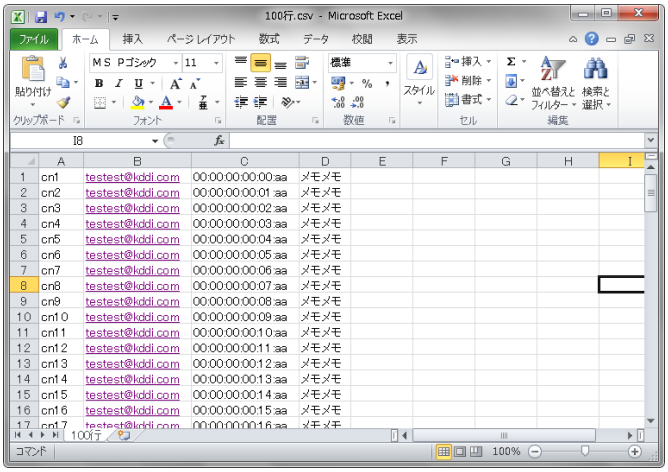
【一括発行申請フォーマット】

※ 1 行目から直接データ領域となります。

※ 最大 500 行まで申請可能です。501 行以上を一括申請する場合は、CSV ファイルを分割して申請ください。

各列の説明は以下のとおりです。

列番号	入力値	入力値の説明
1	CN 値	CN の@よりも左側部分を入力します。(@以下 Suffix 不要)
2	通知先メールアドレス	発行通知メールを送付するメールアドレスを入力します。
3	Auth ID	各デバイスを識別する情報(MAC アドレス /IMEI/UDID/GUID)を入力します。 ※ 1 つの CSV ファイル内で AuthID 種別を混在して入力することはできません。 【MAC アドレスを選択している場合】 xx:xx:xx:xx:xx:xx 形式(半角) 【IMEI を選択している場合】 15 桁の半角数字 【UDID を選択している場合】 40 桁の半角英数字 または 25 桁の半角英数字(9 桁目にハイフンの区切り文字を含む) 【GUID を選択している場合】 32 桁の半角英数字
4	メモ	発行した証明書のメモ情報



【UPN 項目あり】とする場合

UPN のお申し込みが完了し、【証明書の発行申請】において、UPN サフィックス名(@以降)が登録済の場合、一括発行申請時に UPN の値を追加して発行可能です。CSV フォーマットは上記 1～4 の後に、5 番目に UPN の値をご記入ください。また、申請用 CSV ファイルをアップロードする際には、証明書カスタマーコントロールの【証明書の一括発行申請】画面の【UPN 項目あり】にチェックしてください。

列番号	入力値	入力値の説明
1	CN 値	CN の@よりも左側部分を入力します。(@以下 Suffix 不要)
2	通知先メールアドレス	発行通知メールを送付するメールアドレスを入力します。
3	Auth ID	各デバイスを識別する情報(MAC アドレス /IMEI/UDID/GUID)を入力します。 ※ 1 つの CSV ファイル内で AuthID 種別を混在して入力することはできません。 【MAC アドレスを選択している場合】 xx:xx:xx:xx:xx:xx 形式(半角) 【IMEI を選択している場合】 15 桁の半角数字 【UDID を選択している場合】 40 桁の半角英数字 または 25 桁の半角英数字(9 桁目にハイフンの区切り文字を含む)

		【GUID を選択している場合】 32 桁の半角英数字
4	メモ	発行した証明書のメモ情報
5	UPN	UPN の値（UPN ユーザー名+″@″+登録済 UPN サフィックス名の形式）を入力します。

【注意】CSV ファイルは『Shift-JIS』形式の文字コードでアップロードしてください。

【一括失効申請フォーマット】

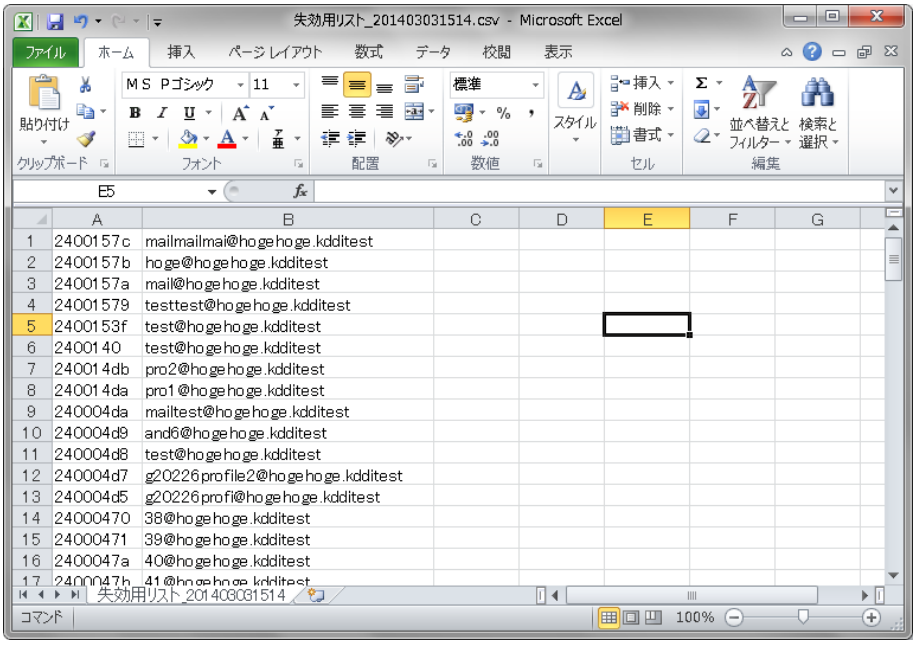
※ 1 行目から直接データ領域となります。

※ 最大 500 行まで申請可能です。501 行以上を一括申請する場合は、CSV ファイルを分割して申請ください。

各列の説明は以下のとおりです。

【注意】申請情報の検索画面から抽出した CSV データフォーマット『失効用 CSV』をなるべく活用ください。
CSV ファイルは『Shift-JIS』形式の文字コードでアップロードしてください

列番号	入力値	入力値の説明
1	シリアル番号	失効対象のシリアル番号を入力します。
2	CN 値	シリアル番号に該当する証明書の CN 値を入力します。 【注意】この CN 値は@suffix 部を含む値となります。



【通知用アドレス一括変更フォーマット】

※ 1 行目から直接データ領域となります。

※ 最大 500 行まで申請可能です。501 行以上を一括申請する場合は、CSV ファイルを分割して申請ください。

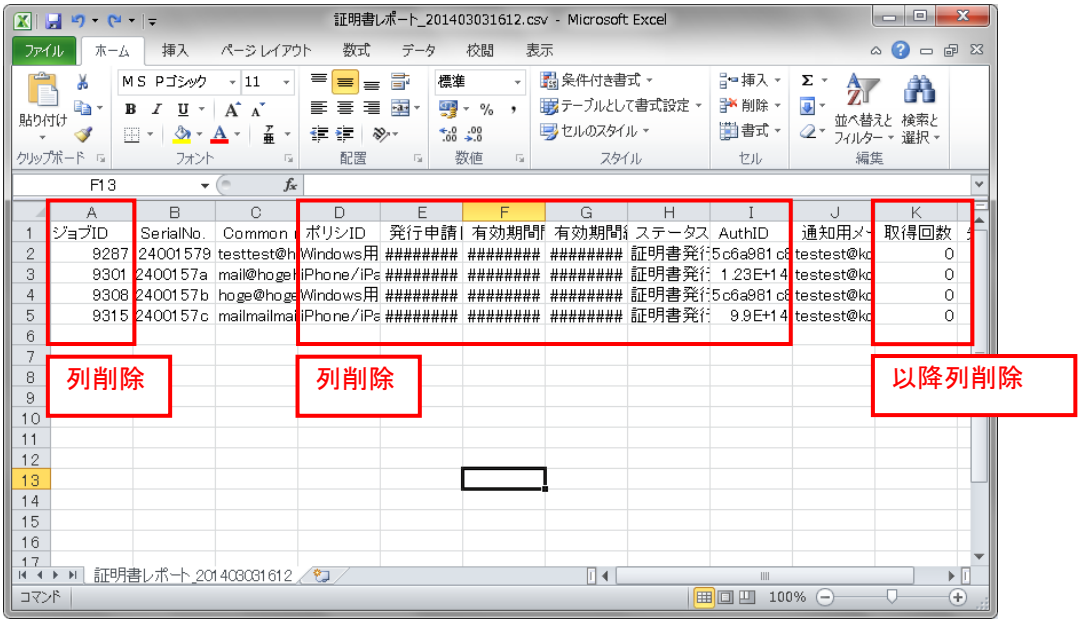
各列の説明は以下のとおりです。

【注意】通知用アドレス一括フォーマットは、申請情報の検索からフォーマットダウンロードすることができません。

列番号	入力値	入力値の説明
1	シリアル番号	証明書シリアル番号
2	CN	証明書シリアル番号に紐付く CN 値(@Suffix 部含む)を入力します。
3	現通知先メールアドレス	過去に発行通知メールを送付しているメールアドレスを入力します。
4	新通知先メールアドレス	今後の処理時に発行通知を送付するメールアドレスを入力します。

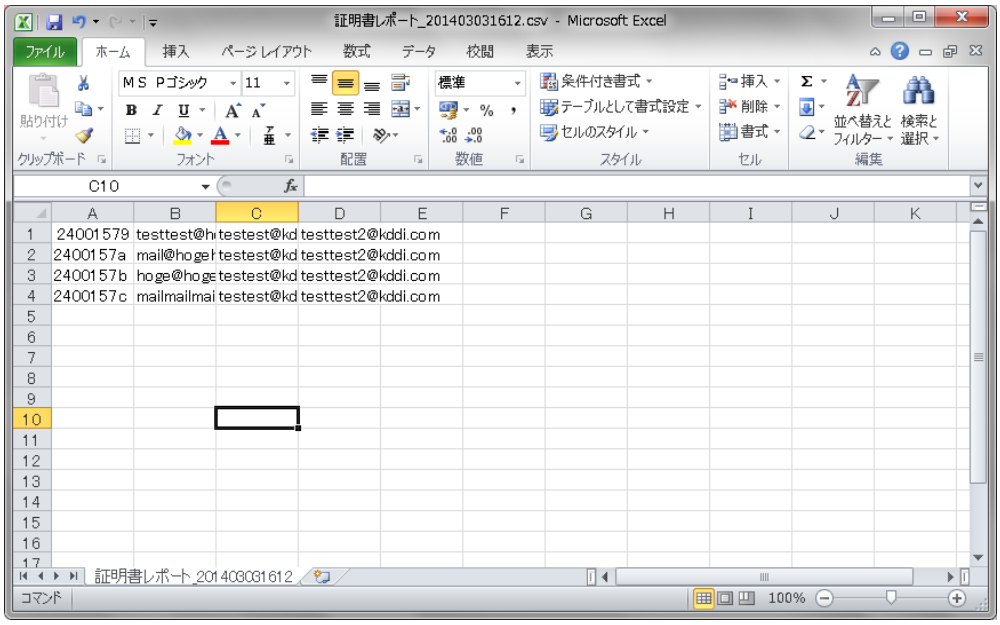
【参考】通知用アドレス一括変更フォーマットの作り方

証明書のレポートをダウンロードします。



不要となる列を削除し、新たな通知先メールアドレス 4 列目に記入します。

1 行目のタイトル行を削除してデータフォーマットが完成します。



【構成プロファイル変更フォーマット】

※ 1 行目から直接データ領域となります。

※ 最大 500 行まで申請可能です。501 行以上を一括申請する場合は、CSV ファイルを分割して申請ください。

各列の説明は以下のとおりです。

列番号	入力値	入力値の説明
1	Auth ID	変更適用する IMEI もしくは UDID 値を入力します。 【注意】同一 CSV 内部 IMEI/UDID 混在はできません。

14 お問い合わせ窓口

【ログイン ID またはパスワードについて】

KDDI 法人営業担当者までお問い合わせください。

【本システムご利用方法】

法人お客さまセンターまでお問い合わせください。

電話:0077-7007(0120-921-919)

受付時間:9:00～18:00 ※ 土・日・祝日・年末年始を除く

【カスタマーコントロールに関する障害/パスワードロック時の解除】

ご利用中 KDDI サービスの受付窓口までご連絡ください。

【KDDI Flex Remote Access】

KDDI サービスコントロールセンター(SCC) 電話:0077-75-010 (0120-911-712)

【KDDI ビジネスセキュア Wi-Fi(標準メニュー)】

KDDI サービスコントロールセンター(SCC) 電話:0120-993-600

【KDDI ビジネスセキュア Wi-Fi(ライトメニュー)】

KDDI サービスコントロールセンター(SCC) 電話:0120-996-001

※ KDDI サービスコントロールセンター(SCC)へのお問い合わせは 24 時間 365 日受付可能です。

※ 個別運用窓口をご利用のお客さまは、各個別運用窓口までご連絡ください。

※ KDDI サービスコントロールセンター(SCC)では、カスタマーコントロールの操作に関わるお問い合わせは対応できかねますので、あらかじめご了承願います。

※ セキュリティを保つため、ロック解除依頼時は、KDDI より Suffix 値(ご契約時に申請された物)とログイン時のログイン ID を確認させていただきます。Suffix 値、ログイン ID の確認が取れない場合は、ロック解除できませんのでご注意ください。Suffix 値・ログイン ID については、開通時にお渡しした『開通のご案内』に記載または、『契約管理システム』内の契約内容照会にて確認できます。

15 定期メンテナンス

KDDI では、以下日時にて定期的にサーバーのメンテナンスを行っております。

この日時でのシステム操作はできませんので、あらかじめご了承願います。

【定期メンテナンス】 毎月第 2 水曜日　22:00～翌 8:00

※ 祝日の場合は翌営業日となります。

※ その他、緊急を要する作業を行う場合がございます。

以上

KDDI 株式会社

【改版履歴】

第 1.0 版（2014 年　3 月 24 日） 初版

第 1.1 版（2014 年　4 月　8 日） 文書内誤記修正、説明内容の拡充

第 1.2 版（2014 年　5 月 29 日） 問い合わせ窓口の修正、メールフォーマット変更、説明内容の拡充

第 1.3 版（2014 年　6 月 20 日） 構成プロファイル登録について追記

第 1.4 版（2014 年　9 月 30 日） メールフォーマット変更、証明書のレポート機能の説明内容の拡充

第 1.5 版（2014 年 10 月 24 日） MAC OS 対応、Windows® Importer 対応、IE10,11 対応

第 1.6 版（2014 年 11 月 12 日） メールフォーマット Android™版の追加

第 1.7 版（2014 年 12 月　9 日） 必要なブラウザ設定に TLS を追記

第 1.8 版（2015 年　1 月 29 日） 管理者アカウントのログインパスワードの文字制限を追記

第 1.9 版（2015 年　4 月 28 日） 失効申請エラーについて注意事項を追記

第 2.0 版（2015 年　8 月 11 日） SHA-2、構成プロファイル簡易作成、通知メールメモ機能の追記

第 2.1 版（2015 年 11 月 20 日） 構成プロファイルの管理について注意事項を追記

第 2.2 版（2016 年　3 月　1 日）「KDDI Flex Remote Access」コンピューターストア証明書対応の修正

第 2.3 版（2016 年　8 月　1 日） Android™注意事項追記

第 2.4 版（2016 年 11 月 16 日） Windows® 10 Mobile・UPN 対応に伴う追記

第 2.5 版（2017 年 4 月 14 日） IE10 サポート終了に伴う修正

第 2.6 版（2017 年 7 月 28 日） Common Name に関する説明を追記

第 2.7 版（2017 年 8 月 7 日） Common Name に関する説明を修正

第 2.8 版（2017 年 9 月 20 日）iOS 版 Cisco AnyConnect 対応に伴い修正

第 2.9 版（2017 年 9 月 29 日）iOS 版 Cisco AnyConnect 対応に伴い構成プロファイルの説明追記

第 3.0 版（2018 年 2 月 8 日） 説明内容拡充。証明書有効期限について追記。

第 3.1 版（2018 年 4 月 16 日） 注意事項追記

第 3.2 版（2018 年 7 月 1 日） ご利用環境に関する説明の追記、

KDDI サービスコントロールセンターへ改称に伴う修正

第 3.3 版（2018 年 11 月 27 日） 有効期間終了通知設定の追加、トップ画面表示変更に伴う修正

第 3.4 版（2019 年 2 月 1 日） Common Name および IMEI に関する注意事項の追記

第 3.5 版（2019 年 4 月 8 日） iOS 版証明書発行通知メールサンプルの修正

第 3.6 版（2019 年 6 月 1 日） 一括発行・失効申請時の CSV フォーマットに関する注意事項の追記

第 3.7 版（2019 年 9 月 11 日） UDID の入力文字制限に関する追記

第 3.8 版（2019 年 9 月 26 日） iPadOS に関する追記

第 3.9 版(2019 年 12 月 12 日） 構成プロファイルの適用アプリに関する追記

第 4.0 版(2019 年 12 月 19 日)Android™10 における証明書インストール方法に関する追記