X-point Cloud

クライアント証明書サービス

管理者マニュアル

2025/11/18 版

ATLED

はじめに

◆本書の目的
本書は、「X-point」のクライアント証明書サービスの運用方法について説明しています。
本書の内容をよくお読み頂いた上で、操作を行なってください。

◆対象とする読者
本書は「X-point」をお使いになる一般ユーザおよびシステム管理者を対象としています。システム管理者とは「X-point」を運用するにあたり必要な設定および基本データの作成、維持管理を行なう本システムの管理権限を持つユーザを指します。

◆対応バージョン（2025/11/18 時点）

X-point	備考
X-point Cloud v3	

◆製品名について
本書中、「X-point サーバ」は「X-point」と表記しています。
また、各製品の名称は対応バージョンを省略してある箇所もありますのでご了承ください。

◆商標について

◆製作著作

目次／索引

1. お使いになる前に

1.1. 対応環境

クライアント証明書サービス(以下、本サービス)で利用するエイトレッド認証局においてクライアント証明書発行業務を行うために、管理者向けに以下の PC 環境(OS、ブラウザ)をご準備いただく必要があります。

【動作環境】

PC 環境	OS： Microsoft Windows 10 / 11 ブラウザ： Firefox、Google Chrome、Microsoft Edge(Chromium 版) （TLS の利用が有効であること） インターネットアクセスが出来る環境

特記事項

本動作環境は、クライアント証明書発行業務のための動作環境です。**X-point のご利用環境とは異なります**ので、ご注意ください。

1.2. エイトレッドから提供されるもの

本サービスをご利用いただくにあたり、エイトレッドはお客様に以下のものをご提供いたします。

納品物が揃っているか、あらかじめご確認ください。

1)開通通知メール

開通通知メールには以下が記載されています。

・エイトレッド認証局 URL

・ログイン ID

・ログインパスワード

・認証局ログイン用証明書（添付）

・認証局ログイン用証明書パスワード

開通通知は、クライアント証明書サービスの開通日にエイトレッドからメールにて通知されます。

1.3. 本書における用語説明

本書をお読みいただくにあたり、基本的な用語の説明を下表に示します。

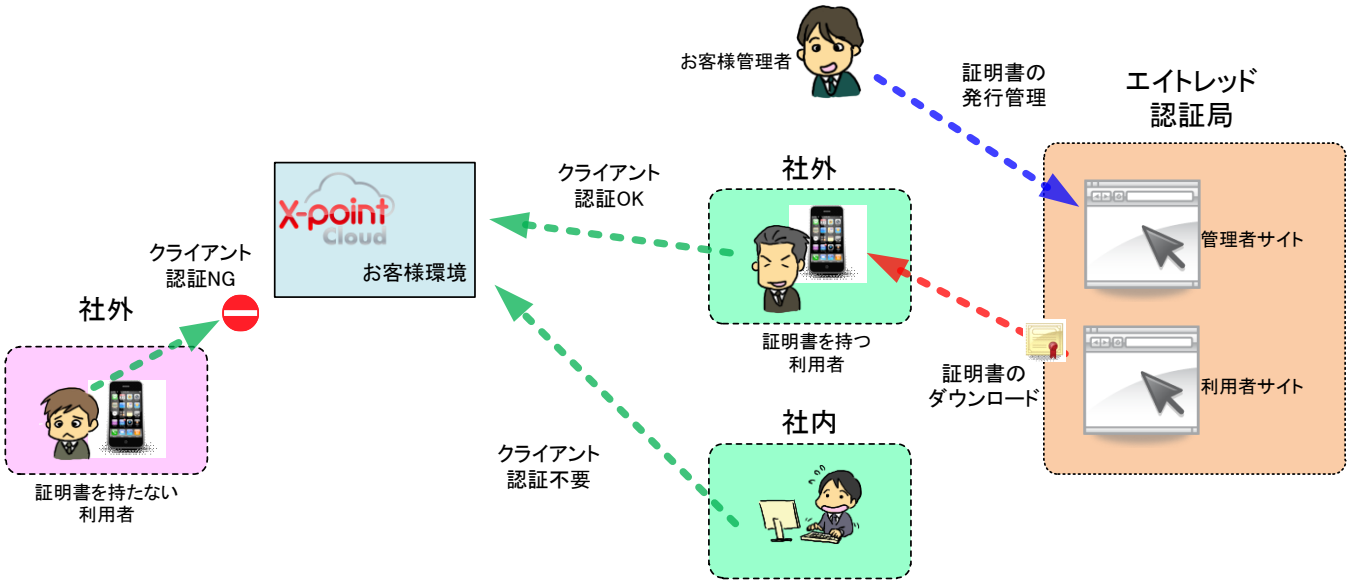
用語	内容
エイトレッド認証局	クライアント証明書サービスで利用されるクライアント証明書の発行管理から配布までを行うシステム全般の総称です。 **本書において特に断りがない場合、「認証局」は「エイトレッド認証局」のことを指します。**
管理者	クライアント証明書サービスを利用する権限を持つ、お客様側の管理者を指します。 管理者にはエイトレッド認証局の操作以外に次の役割をお願いいたします。 ・　証明書利用者へ、証明書の発行に必要な情報を通知する
デバイス	本書では実際に証明書を使用する端末全般（PC、スマートフォン、タブレット等）を指します。
認証局ログイン用証明書 （管理者証明書）	管理者がエイトレッド認証局へログインする際の SSL クライアント認証のために使用する証明書です。認証局ログイン用証明書は開通通知メールに添付します。
クライアント証明書 （デバイス証明書）	証明書利用デバイスに格納される証明書を指します。 この証明書を使用して、X-point サービス接続時の認証を行います。 **本書において特に断りがない場合、「証明書」は「クライアント証明書」のことを指します。**
ログイン ID,パスワード	管理者がエイトレッド認証局へログインする際に必要な ID とパスワードです。ログイン証明用証明書は開通通知メールに記載します。
ユーザ名、ユーザパスワード	利用者がクライアント証明書をダウンロードするためのサイトにログインするために必要な ID とパスワードです。
CRL(失効リスト)	Certificate Revocation List の略称で、無効化したクライアント証明書のリストです。
PKCS#12	エイトレッド認証局から証明書をファイルとしてダウンロードした時の形式の名前です。 証明書と秘密鍵がパッケージされ、パスワードにより保護されています。

2. クライアント証明書サービス

2.1. 利用イメージ

クライアント証明書サービス(以下、本サービス)とは、クライアント証明書による認証機構を利用することにより、X-point Cloud に接続できるデバイスを制限するためのサービスです。本サービスをご契約されますと、エイトレッド認証局で発行したクライアント証明書をインストールした特定のデバイスのみが X-point Cloud にアクセス可能となり、高度なセキュリティを確保することが可能となります。

また、本サービスではお客様ご自身がエイトレッド認証局でクライアント証明書を発行し、各利用者に配布することができます。



2.2. クライアント証明書サービス仕様

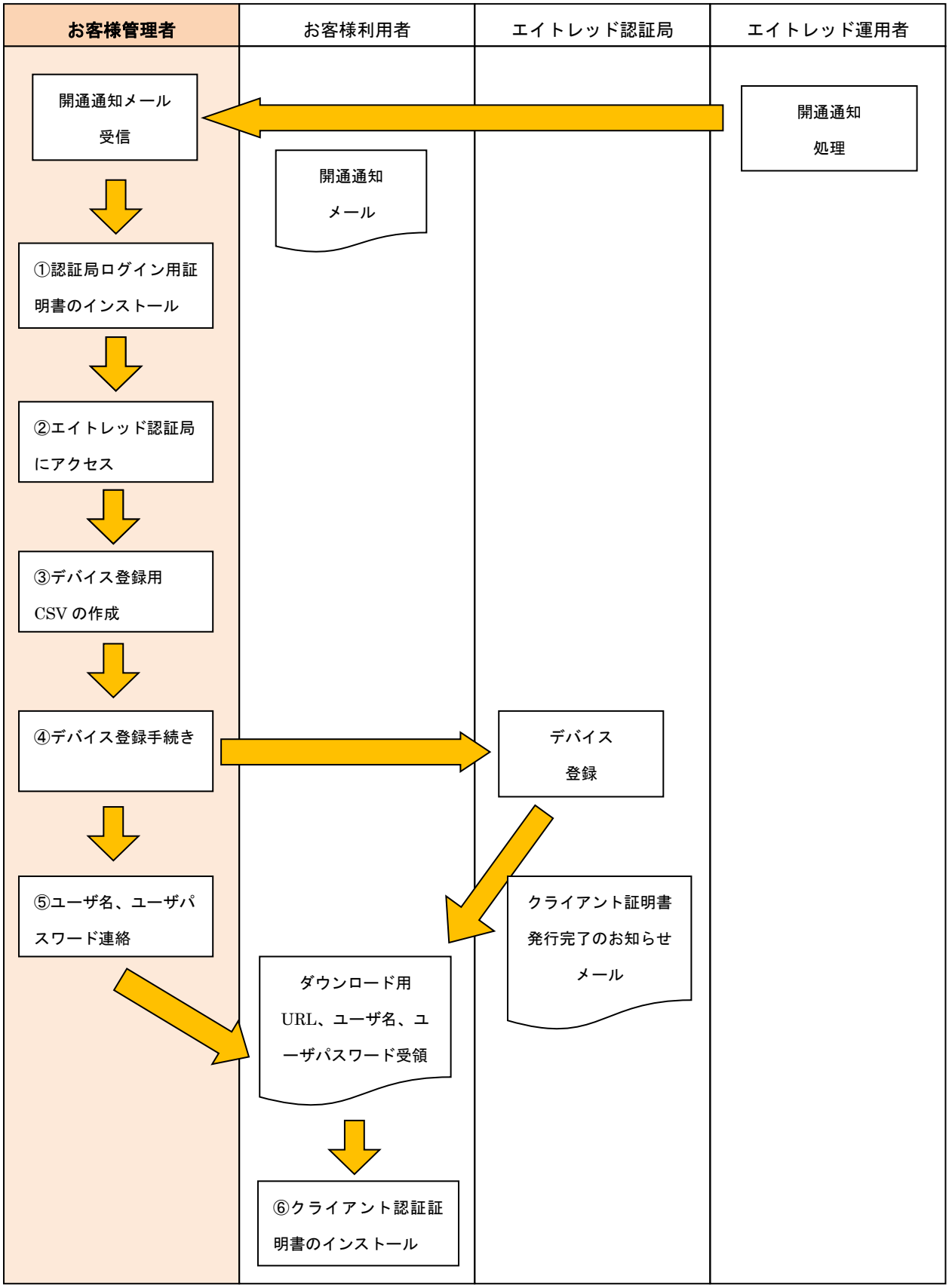
エイトレッドが提供するクライアント証明書サービスの主な仕様は以下の通りです。

また、エイトレッド認証局は株式会社インテック社の「EINS/PKI+ for Smart Device」を利用しています。

利用用途	X-point Cloud デバイス認証
鍵長	2048bit
暗号強度	256bit
暗号アルゴリズム	RSA
ダイジェストアルゴリズム	SHA-256
有効期間	365 日
CRL 更新周期	24 時間

2.3. ご利用までの基本的な流れ

本サービス利用開始からクライアント証明書のインストールまでの流れを下記に記載します。



2.4. 前提条件・制限事項等

2.4.1. 運用時間

エイトレッド認証局は CRL(失効リスト)を更新するため、毎日 AM0:00～0:30 の間メンテナンス停止します。
この間はお客様管理者による証明書の発行業務が行えませんが、X-point 自体のご利用には影響ありません。
また、このほかにもエイトレッドの運用計画に基づき、メンテナンスが発生する場合があります。

2.4.2. CRL(失効リスト)更新

X-point サービスの失効リストは一日一回(AM2:00)の更新となります。この失効リスト更新の際、X-point サービスの瞬断が発生する可能性があります。なお、バックアップやクエリ自動出力などのバッチ処理が停止することはありません。

2.4.3. クライアント認証ライセンス

本サービスをご契約いただきますと、お客様社外から X-point Cloud を利用するデバイスと同数のクライアント認証ライセンスが必要で、社外からアクセスするすべての端末にクライアント証明書をインストールする必要があります。

2.4.4. 各サービスとの併用

本サービスは以下の機能／オプション／サービスと併用できません。

・X-point のゲストフォーム（X-point 標準機能）

また、デバイスによってグループウェア連携サービスに制限事項がございます。詳細につきましては、以下の URL の動作環境をご確認ください。

【X-point Cloud 動作環境】
https://www.atled.jp/document/xpoint/version_xpcloudv3.html

2.4.5. IP 接続制限サービスについて

本サービスは、IP 接続制限サービスと併用することを前提としております。お客様のご利用拠点(事務所等)は固定のグローバル IP によるインターネット接続を行っている必要があります。固定のグローバル IP 接続につきまして、詳しくはインターネットサービスプロバイダまでご相談ください。固定のグローバル IP を持たずに本サービスをご利用される場合、X-point Cloud に接続するすべての端末数分のクライアント証明書が必要になります。

2.4.6. SharePoint 連携サービスとの併用

本サービスと SharePoint 連携サービスを併用してご利用いただく場合、SharePoint に設定する WEB パーツのパラメータスコープには「GET」を指定してください。
その他、SharePoint 連携の設定方法につきましては、マニュアル「SharePoint 連携アダプタ 導入・設定ガイド」をご確認ください。

2.4.7. Google Apps 連携サービスとの併用

本サービスと Google Apps 連携サービスを併用してご利用いただく場合、マニュアル「Google Apps 連携アダプタ 導入・設定ガイド」にそって連携設定を行った後、追加の設定が必要となります。

1) Google Developer Console へログインします。

2) 「認証情報」メニューから、マニュアル「Google Apps 連携アダプタ 導入・設定ガイド」で追加した名称の「OAuth 2.0 クライアント ID」を選択してください。

3) 「承認済みのリダイレクト URI」の空欄のボックスに以下のサンプルの URL を参考に入力して、「保存」をクリックします。

■連携マニュアルにしたがって追加した URL
https://xp999999ab.atledcloud.jp/xpoint/googleAuth

■追加で設定する URL
https://xp999999ab-cl.atledcloud.jp/xpoint/googleAuth

ホスト名の部分に“-cl”(ハイフン・シー・エル)を付与した URL となります。

2.5. 事前準備

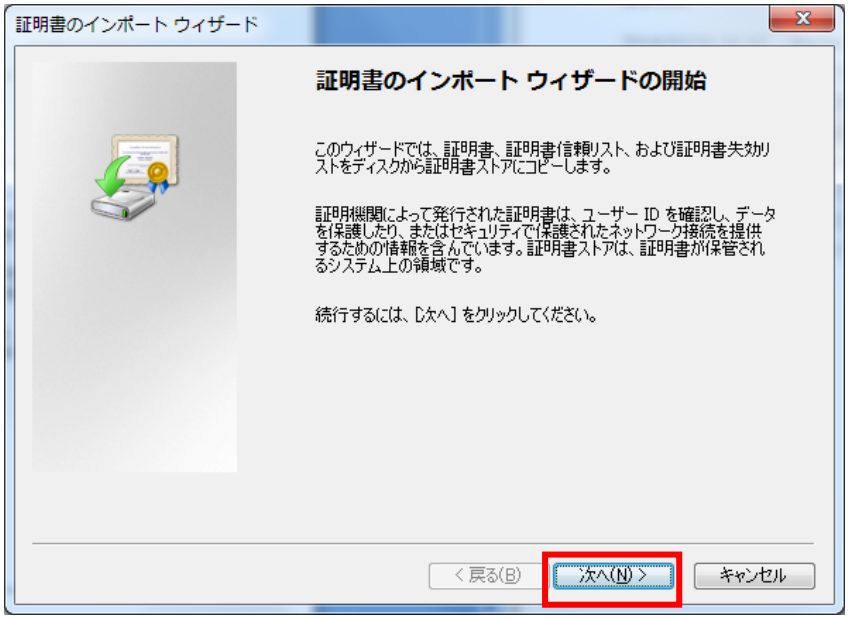
2.5.1. 認証局ログイン用の証明書のインストール

エイトレッド認証局にアクセスするためには、ログイン用の証明書(認証局ログイン用証明書)をインストールして頂く必要がございます。この手順は、実際にエイトレッド認証局で証明書発行業務を行う管理者がご利用するデバイスで実施してください。

特記事項

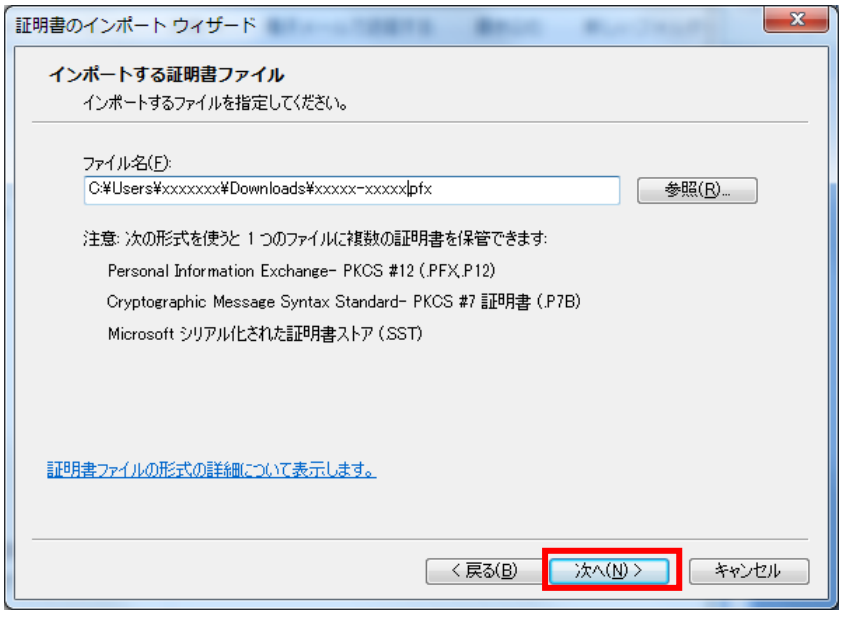
本手順は初めてエイトレッド認証局にアクセスする場合または PC を変更した時のみ必要です。認証局ログイン用証明書は複数の端末にインストール可能です。

1)開通通知にて添付されていた証明書ファイル（pfx ファイル）をダブルクリックします。



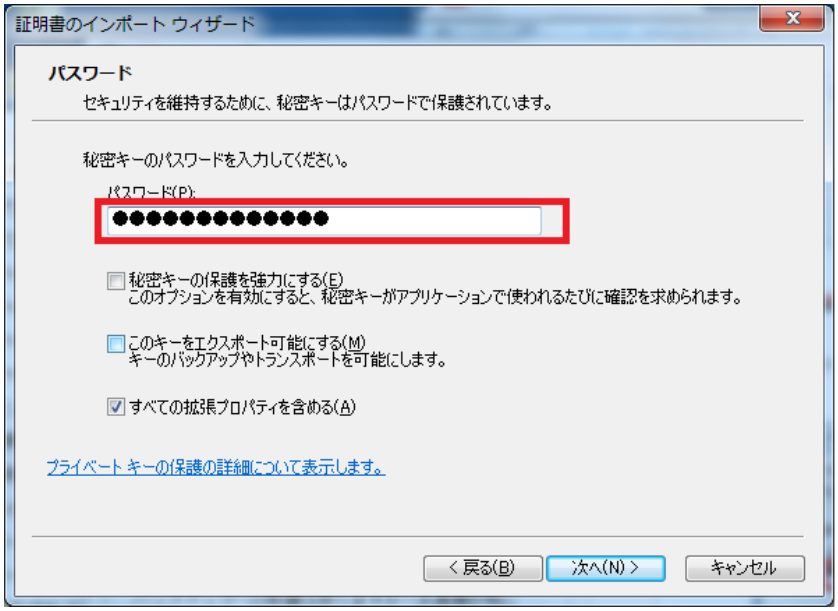
「次へ(N)>」をクリックします。

2)インポートする証明書ファイル



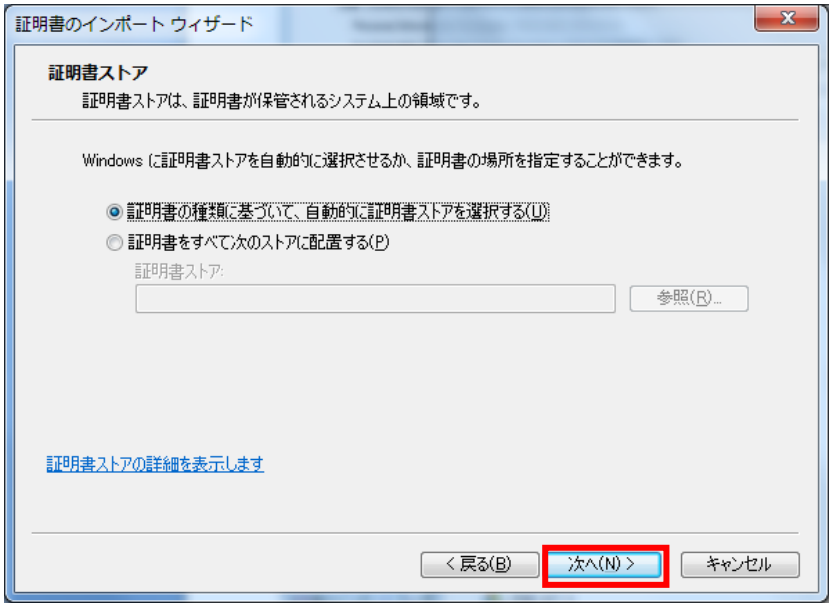
何も変更せずに、
「次へ(N)>」をクリックします。

3)インポートする証明書ファイル



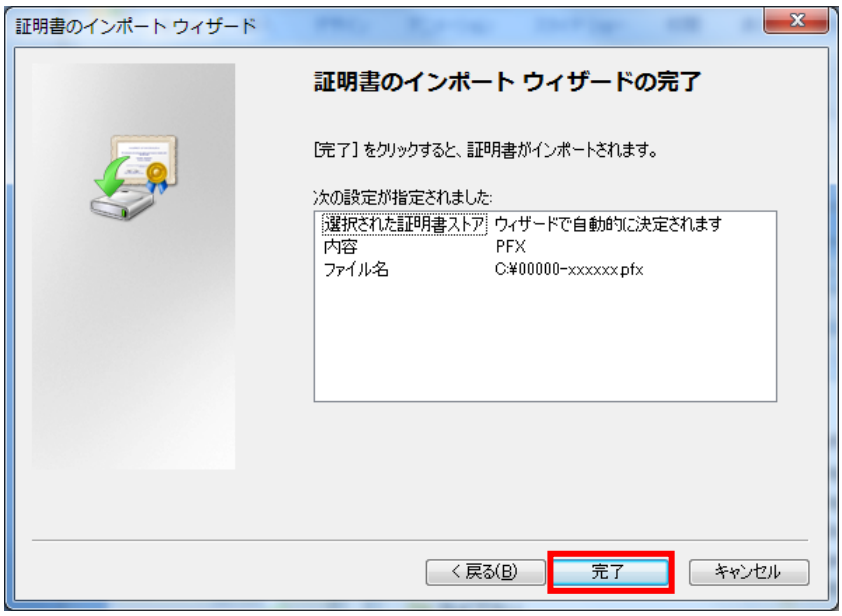
「パスワード(P)」に開通通知メールに記載してある「認証局ログイン用証明書パスワード」を入力して、「次へ(N)>」をクリックします。

4)証明書ストア



「証明書の種類に基づいて、自動的に証明書ストアを選択する(U)」にチェックが付いていることを確認して、「次へ(N)>」をクリックします。

5)証明書のインポートウィザードの完了

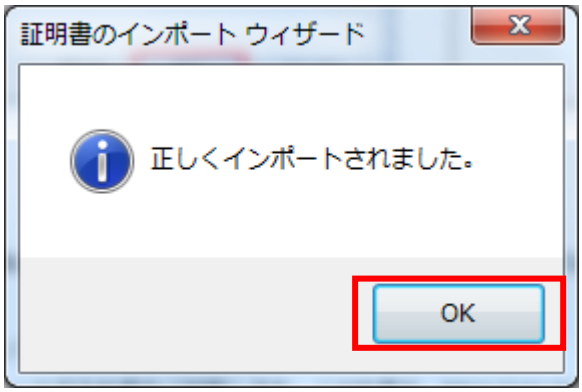


「完了」をクリックします。

特記事項

「完了」クリック後にセキュリティ警告「発行者が次であると主張する証明書機関(CA)から証明書をインストールしようとしています：」が表示された場合は、「はい(Y)」をクリックしてください。

6)証明書のインポート完了



「OK」をクリックします。

2.6. エイトレッド認証局

エイトレッド認証局でクライアント証明書発行業務に必要な画面構成と機能概要をご説明いたします。

※本マニュアルでは発行業務に必要な機能のみをご説明していきます。

2.6.1. ログイン画面

エイトレッド認証局管理画面にログインする方法を以下にご説明いたします。これは、エイトレッド認証局をご利用いただくための基本操作となります。

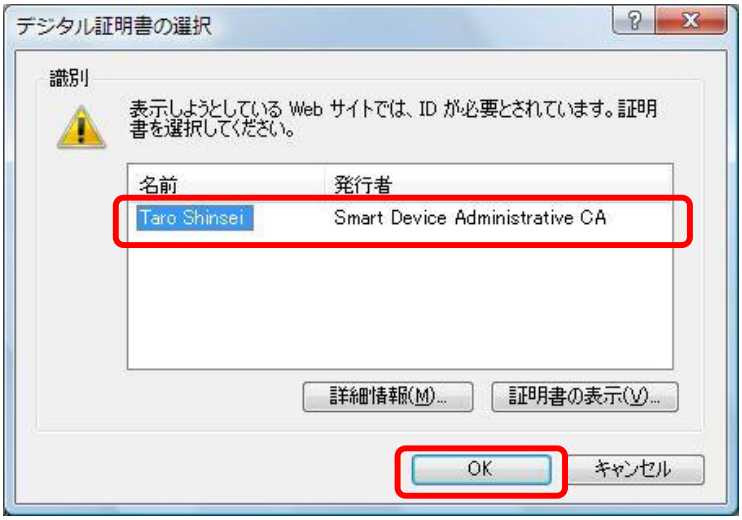
1) ブラウザで以下の URL にアクセスします。

https://smadev.einspki.jp/

2) 証明書の選択画面が表示されます。認証局ログイン用証明書を選択して「OK」を押してください。

なお、クライアント証明書をインストールすると、ご利用環境によっては複数の証明書が表示される場合があります。

エイトレッド認証局にアクセスする場合は、名前が開通通知メールに記載されているログイン ID と同じものを選択してください



3) 認証に成功すると次のログイン画面が表示されますので、開通通知メールに記載されている「ログイン ID」、「パスワード」を入力して「ログイン」ボタンを押してください。

2.6.2. 機能説明

2.6.2.1. 機能説明（デバイス管理）

ログイン後の TOP 画面となります。

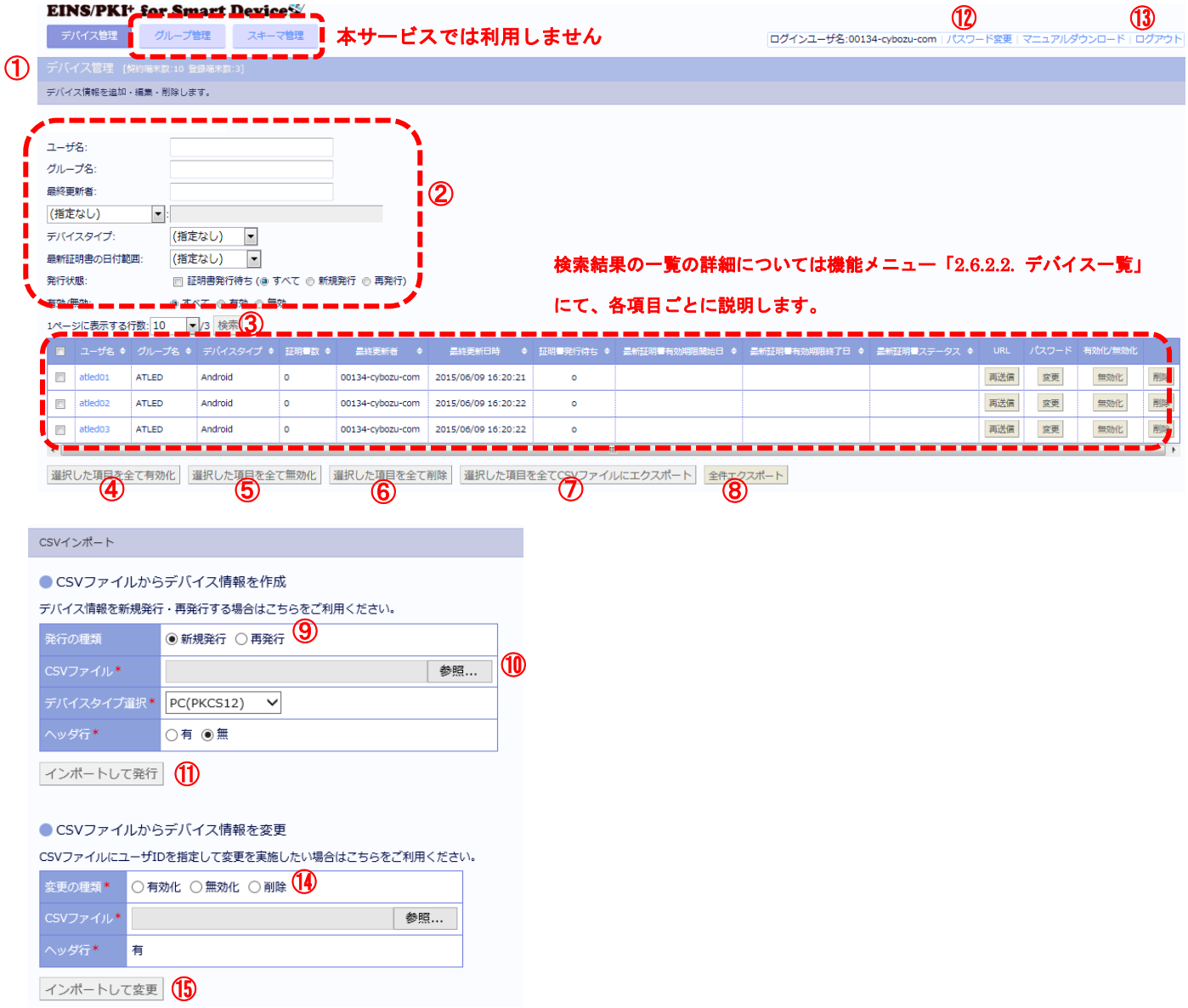


図　2.6.2-1 デバイス管理

表 2.6.2-1　デバイス管理項目説明

	項目名	説明	備考
①	契約端末数／ 登録端末数	ご契約いただいていているクライアント証明書サービスのライセンス数と現在登録されているライセンス数を表示します。	契約ライセンス数を超える登録はできません。
②	証明書検索条件	証明書の検索条件を指定します。	
③	【検索】ボタン	デバイス情報を検索します。 条件に該当したデバイスの一覧が表示されます。デバイス一覧では、証明書発行対象のユーザ、発行日、有効期限などの情報を参照することが可能です。 詳細については、次ページをご覧ください。	大文字小文字は区別されます。 検索パターンは部分一致です。
④	【選択した項目を全て有効化】ボタン	チェックボックスで選択されたデバイスの有効/無効状態をすべて有効化します。	
⑤	【選択した項目を全て無効化】ボタン	チェックボックスで選択されたデバイスの有効/無効状態をすべて無効化します。	
⑥	【選択した項目を全て削除】ボタン	チェックボックスで選択されたデバイスをすべて削除します。	
⑦	【選択した項目を全て CSV ファイルにエクスポート】ボタン	チェックボックスで選択されたデバイスの情報を CSV 形式でエクスポートします。	
⑧	【全件エクスポート】ボタン	登録されている全てのデバイス情報を CSV 形式でエクスポートします。	
⑨	【新規発行/再発行】ラジオボタン	証明書発行の種類を選択します。	
⑩	【デバイスタイプ選択】プルダウン	プルダウンで選択されたデバイスを選択します。	
⑪	【インポート】ボタン	CSV ファイルをインポートすることで、デバイス情報を登録します。	
⑫	【パスワード変更】ボタン	管理者のパスワードを変更します。	
⑬	【ログアウト】ボタン	管理者サイトをログアウトします。	
⑭	【変更の種類】ラジオボタン	デバイスの有効化、無効化、削除を選択します。	
⑮	【インポートして変更】ボタン	CSV ファイルをインポートすることで一括でデバイスの有効化、無効化、削除を行います。	

2.6.2.2.　　機能説明（デバイス一覧）

デバイス一覧の初期表示の並び順は作成日時の降順となります。

並び順を変更する場合は、各項目の上下矢印をクリックしてください。

図　2.6.2-2 デバイス一覧

表 2.6.2-2　デバイス一覧項目説明

	項目名	説明	備考
①	【ユーザ名】リンク	デバイスの詳細情報を表示します。	
②	証明書数	現在までに発行された証明書の総枚数を表示します。	有効期限切れ等で再発行した場合も総数に含まれます。
③	証明書発行待ち	証明書の発行状態を表示します。	デバイスの登録後、クライアント証明書が発行待ちであれば「o」が表示されます。 証明書が発行済みであればブランクが表示されます。
④	最新証明書有効期限開始日	当該デバイスの最新証明書の有効期限開始日を表示します。	証明書が期限切れしている場合でも、直近で発行した証明書の有効期限開始日が表示されます。
⑤	最新証明書有効期限終了日	当該デバイスの最新証明書の有効期限終了日を表示します。	同上
⑥	最新証明書ステータス	当該デバイスの最新証明書のステータス（発行済み、失効済み、有効期限切れ）を表示します。	
⑦	【再送信】ボタン	証明書発行画面の URL をメール/SMS で再送信します。	デバイスタイプが「PC(PKCS12)」、「IE (UserStore)」の場合にボタンが表示されます。
⑧	【変更】ボタン	対象のデバイスが証明書発行する際に使用するパスワードを変更します。	パスワードに指定できる文字列は以下の通りです。 ・1 文字以上の半角英数字記号 ※詳細は「3.2.1 デバイス登録用の CSV を準備する」をご確認ください。
⑨	【無効化】ボタン	対象のデバイスを無効にします。	証明書発行画面へのアクセス、プロファイル再適用、URL 再送信が使用できなくなります。 **証明書が無効化されて、失効リストに記載されます。また、無効化するとボタンが【有効化】に変わります。**
	【有効化】ボタン	無効にしたデバイスを有効にします。	**証明書が有効化されて、失効リストが除外されます。また、有効化するとボタンが【無効化】に変わります。**
⑩	【削除】ボタン	対象のデバイスを削除します。	デバイス一覧から当該デバイスの情報が削除されます。なお、1 度削除したデバイス情報はもとに戻すことはできません。再度利用する場合は、デバイスの新規登録を行ってください。 **発行済の証明書が存在する場合、証明書が失効されます。**

2.6.2.3. 機能説明（デバイス詳細/デバイス）

デバイス一覧で【ユーザ名】リンクをクリックすると、デバイスの詳細情報が表示されます。詳細情報は以下のカテゴリに分けられます。

- デバイス

  デバイスに関する情報が表示されます。デバイスの状態に係わらず表示されます。

- 通知

  証明書発行 URL の通知に関する情報が表示されます。当該デバイスが属するグループにおいて、URL 通知が指定されている場合に表示されます。

- 証明書

  証明書に関する情報が表示されます。証明書を一枚でも発行している場合に表示されます。

デバイス詳細

デバイス	
ユーザ名	atled01
グループ名	ATLED
端末製品名	
デバイスタイプ	Android
証明書数	0
最終更新者	00134-cybozu-com
最終更新日時	2015/06/09 16:20:21
証明書発行待ち	o
最新証明書有効期限開始日	
最新証明書有効期限終了日	
最新証明書ステータス	
有効/無効	有効
メールアドレス	atled01@atled.jp
電話番号	
電話キャリア	
アクセスURL	https://api.einspki.jp/android/login/JAMAIlLReX
UDID/ANDROID_ID	
IMEI	
ICCID	
MEID	
シリアル番号	
MACアドレス	
デバイス名	
製品名	
バージョン	
表示言語	
付加情報1	
付加情報2	
付加情報3	
付加情報4	
付加情報5	
認証項目	

図 2.6.2-3　デバイス詳細画面（デバイス）

表 2.6.2-3　デバイス詳細画面（デバイス）項目説明

項目	説明
ユーザ名	CSV ファイルで指定したユーザ名
グループ名	デフォルト「ATLED」が表示されます。
端末製品名	※本サービスでは表示されません。
デバイスタイプ	CSV ファイルアップロード時に選択したデバイスの OS の種類
証明書数	現在までに発行された証明書の総枚数
最終更新者	デバイス情報の最終更新管理者名
最終更新日時	デバイス情報の最終更新日時
証明書発行待ち	証明書の発行状態 ・新規・更新発行待ち：o ・証明書が発行済：ブランク
最新証明書有効期限開始日	当該デバイスの最新証明書の有効期限開始日時 有効期限が切れている場合は直近で発行した証明書の有効期限開始日です。
最新証明書有効期限終了日	当該デバイスの最新証明書の有効期限終了日時 有効期限が切れている場合は直近で発行した証明書の有効期限終了日です。
最新証明書ステータス	当該デバイスの最新証明書のステータス（発行済み、失効済み、有効期限切れ）
有効/無効	デバイス情報が有効か無効化を表示
メールアドレス	CSV ファイルで指定したメールアドレス
電話番号	※本サービスでは表示されません。
電話キャリア	※本サービスでは表示されません。
アクセス URL	証明書発行ページの URL
UDID/ANDROID_ID	※本サービスでは表示されません。
IMEI	※本サービスでは表示されません。
ICCID	※本サービスでは表示されません。
MEID	※本サービスでは表示されません。
シリアル番号	※本サービスでは表示されません。
MAC アドレス	※本サービスでは表示されません。
デバイス名	※本サービスでは表示されません。
製品名	※本サービスでは表示されません。
バージョン	※本サービスでは表示されません。
表示言語	※本サービスでは表示されません。
付加情報 1～5	※本サービスでは表示されません。
認証項目	※本サービスでは表示されません。

2.6.2.4. 機能説明（デバイス詳細/通知）

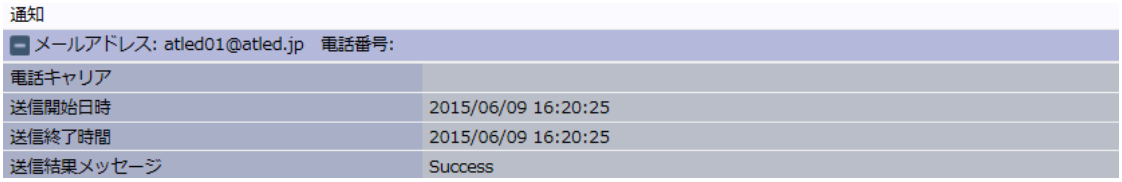
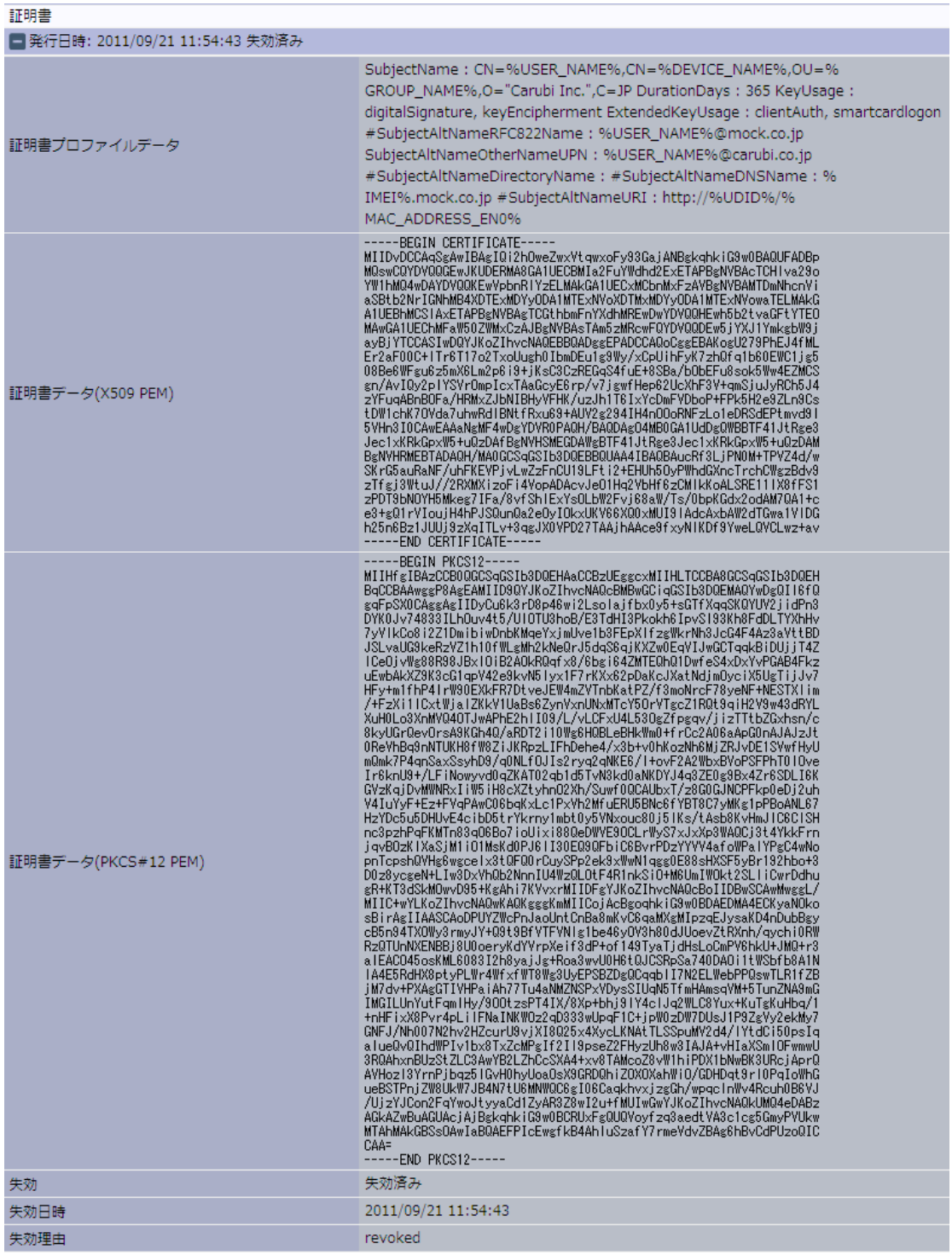


図 2.6.2-4 デバイス詳細画面（通知）

表 2.6.2-4 デバイス詳細画面（通知）項目説明

項目	説明
メールアドレス	ユーザのメールアドレス
電話番号	※本サービスでは表示されません。
電話キャリア	※本サービスでは表示されません。
送信開始日時	送信が開始された日時
送信終了時間	送信が終了した日時
送信結果メッセージ	URL 通知をした結果のメッセージ

2.6.2.5.　　機能説明（デバイス詳細/証明書）



証明書	
発行日時: 2011/09/21 11:54:43 失効済み	
証明書プロファイルデータ	SubjectName：CN=%USER_NAME%,CN=%DEVICE_NAME%,OU=%GROUP_NAME%,O="Carubi Inc.",C=JP DurationDays：365 KeyUsage：digitalSignature, keyEncipherment ExtendedKeyUsage：clientAuth, smartcardlogon #SubjectAltNameRFC822Name：%USER_NAME%@mock.co.jp SubjectAltNameOtherNameUPN：%USER_NAME%@carubi.co.jp #SubjectAltNameDirectoryName：#SubjectAltNameDNSName：%IMEI%.mock.co.jp #SubjectAltNameURI：http://%UDID%/%MAC_ADDRESS_EN0%
証明書データ(X509 PEM)	-----BEGIN CERTIFICATE----- MIIDvDCCAqSgAwIBAgIQi2hOweZwxYtqwxoFy93GajANBgkqhkiG9w0BAQUFADBp MQswCQYDVQQGEwJKUDERMA8GA1UECBMIa2FuYWdhd2ExETAPBgNVBAcTCHIva29o YW1hMQ4wDAYDVQQKEwVpbnRlYzELMAkGA1UECxMCbnMxFzAVBgNVBAMTDmNhcnVi aSBtb2NrIGNhMB4XDTExMDYyODA1MTExNVoXDTMxMDYyODA1MTExNVowaTELMAkG A1UEBhMCSIAxETAPBgNVBAgTCGthbmFnYXdhMREwDwYDVQQHEwh6b2tvaGFtYTEO MAwGA1UEChMFaW50ZWMxCzAJBgNVBAsTAm5zMRcwFQYDVQQDEw5jYXJ1YmkgbW9j ayBjYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKogU279PhEJ4fML Er2aFO0C+lTr6T17o2TxoUugh0IbmDEu1g9Wy/xCpUihFyK7zh0fq1b60EWC1jg5 08Be6WFgu6z5mX6Lm2p6i9+jKsC3CzREGqS4fuE+8SBa/bObEFu8sok5Ww4EZMCS gn/AvIQy2plYSYrOmpIcxTAaGcyE6rp/v7jgwfHep62UcXhF3V+qmSjuJyRCh5J4 zYFuqABnBOFa/HRMxZJbNIBHyVFHK/uzJh1T6IxYcDmFVDboP+FPk5H2e9ZLn3Cs tDW1chK7OVda7uhwRdlBNtfRxu89+AUV2g294IH4nOOoRNFzLo1eDRSdEPtmvd9I 5VHn3IOCAwEAAaNgMF4wDgYDVR0PAQH/BAQDAgO4MB0GA1UdDgQWBBTF41JtRge3 Jec1xKRkGpxW5+uQzDAfBgNVHSMEGDAWgBTF41JtRge3Jec1xKRkGpxW5+uQzDAM BgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBAucRf3LjPN0M+TPVZ4d/w SKrG5auRaNF/uhFKEVPjvLwZzFnCU19LFti2+EHUh5OyPWhdGXncTrchCWgzBdv9 zTfgj3WtuJ//2RXMXizoFi4VopADAcvJeO1Hq2YbHf8zCMlkKoALSRE11lX8fFS1 zPDT9bNOYH5Mkeg7IFa/8vfShlExYsOLbW2Fvj88aW/Ts/0bpKGdx2odAM7QA1+c e3+gQ1rVIoujH4hPJSQunQa2eOyIOkxUKV66XQOxMUI9lAdcAxbAW2dTGwa1VlDG h25n6Bz1JUUj9zXqITLv+3qgJX0YPD27TAAjhAAce9fxyNlKDf9YweLQYCLwz+av -----END CERTIFICATE-----
証明書データ(PKCS#12 PEM)	-----BEGIN PKCS12----- MIIHfgIBAzCCB0QGCSqGSIb3DQEHAaCCBzUEggcxMIIHLTCCBA8GCSqGSIb3DQEH BqCCBAAwggP8AgEAMIID9QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIl6fQ gqFpSXOCAggAgIIDyCu6k3rD8p46wi2Lsolajfbx0y5+sGTfXqqSKQYUV2jidPn3 DYKOJv74833ILhOuv4t5/UlOTU3hoB/E3TdHI3Pkokh6IpvSI93Kh8FdDLTYXhHv 7yVlkCo8i2Z1DmibiwDnbKMqeYxjmUve1b3FEpXlfzgWkrNh3JcG4F4Az3aYttBD JSLvaUG9keRzVZ1h1OfWLgMh2kNeQrJ5dqS8qjKXZw0EqYIJwGCTqqkBiDUjjT4Z lCeOjvWg88R98JBxlOiB2AOkRQqfx8/6bgi64ZMTEOhQ1DwfeS4xDxYvPGAB4Fkz uEwbAkXZ9K3cG1qpV42e9kvN5lyx1F7rKXx62pDaKcJXatNdjmOyciX5UgTijJv7 HFy+m1fhP4lrW9OEXkFR7DtveJEW4mZVTnbKatPZ/f3moNrcF78yeNF+NESTXlim /+FzXi1lCxtWjalZKkV1UaBs6ZynVxnUNxMTcY5OrYTgcZ1RQt9qiH2V9w43dRYL XuHOLo3XnMVQ4OTJwAPhE2hlIO9/L/vLCFxU4L53OgZfpgqv/jizTTtbZGxhsn/c 8kyUGr0ev0rsA9KGh4Q/aRDT2i1OWg6HQBLeBHkWm0+frCc2A08aApGOnAJAJzJt OReVhBq9nNTUKH8fW8ZiJKRpzLIFhDehe4/x3b+v0hKozNh6MjZRJvDE1SYwfHyU m0mk7P4qnSaxSsyhD9/q0NLfOJIs2ryq2qNKE6/l+ovF2A2WbxBVoPSFPhT0lOve Ir6knU9+/LFiNowyvd0qZKAT02qb1d5TvN3kd0aNKDYJ4q3ZE0g9Bx4Zr6SDLI6K GVzKqjDvMWNRxIiW5iH8cXZtyhnO2Xh/SuwfQQCAUbxT/z8GOGJNCPFkp0eDj2uh Y4IuYyF+Ez+FVqPAwCO6bqKxLc1PxVh2MfuERU5BNc6fYBT8C7yMKg1pPBoANL67 HzYDc5u5DHUvE4cibD5trYkrny1mbtOy5YNxouc80j5lKs/tAsb8KvHmJlC6ClSH nc3pzhPqFkMTn83qO6Bo7ioUixi88QeDWVE9OCLrWyS7xJxXp3WAQCj3t4YkkFrn jqvBOzKlXaSjM1iO1MsKd0PJ6lI3OEQ9QFbiC6BvrPDzYYV4afoWPalYPgC4wNo pnTcpshQVHg8wgceIx3tQFQ0rCuySPp2ek9xWwN1qgg0E88sHXSF5yBr192hbo+3 D0z8ycgeN+LIw3DxVhQb2NnnIU4WzOLOtF4R1nkSiO+M6UmIWOkt2SLliCwrDdhu gR+KT3dSkMOvvD95+KgAhi7KYvxrMIIDFgYJKoZIhvcNAQcBoIIDBwSCAwMwggL/ MIIC+wYLKoZIhvcNAQwKAQKgggKmMIICojAcBgoqhkiG9w0BDAEDMA4ECKyaNOko sBirAgIIAASCAoDPUYZWcPnJaoUntCnBa8mKvC8qaMXgMIpzqEJysaKD4nDubBgy cB5n94TXOWy3rmyJY+O9t9BfVTFVNlg1be46yOV3h80dJUoevZtRXnh/qychiORW RzQTUnNXENBBj8UOoeryKdYYrpXeif3dP+of149TyaTjdHsLoCmPV6hkU+JMO+r3 aIEACO45osKML6083I2h8yajJg+Roa3wvU0H6tQJCSRpSa740DAOi1tWSbfb8A1N lA4E5RdHX8ptyPLWr4WfxfWT8Wg3UyEPSBZDgQCqqblI7N2ELWebPPQswTLR1fZB jM7dv+PXAgGTIVHPaiAh77Tu4aNMZNSPxVDysSIUqN5TfmHAmsqYM+5TunZNA9mG IMGILUnYutFqmlHy/9OOtzsPT4IX/8Xp+bhj8lY4clJq2WLC8Yux+KuTgKuHbq/1 +nHFixX8Pvr4pLiIFNaINKWOz2qD333wUpqF1C+jpW0zDW7DUsJ1P9ZgYy2ekMy7 GNFJ/Nh0O7N2hv2HZcurU9vjXI8Q25x4XycLKNAtTLSSpuMV2d4/lYtdCi50psIq aIueQvQIhdWPIv1bx8TxZcMPgIf2Il9pseZ2FHyzUh8w3IAJA+vHIaXSmlOFwmwU 3RQAhxnBUzStZLC3AwYB2LZhCcSXA4+xv8TAMcoZ8vW1hiPDX1bNwBK3URcjAprQ AYHozl3YrnPjbqz5lGvHOhyUoaOsX9GRDQhiZOXOXahWiO/GDHDqt9rlOPqIoWhG ueBSTPnjZW8UkW7JB4N7tU8MNWOC6gI06CagkhvxjzgGh/wpqclnWv4RcuhOB8YJ /UjzYJCon2FqYwoJtyyaCd1ZyAR3Z8wI2u+fMUIwGwYJKoZIhvcNAQkUMQ4eDABz AGkAZwBuAGUAcjAjBgkqhkiG9w0BCRUxFgQUQYoyfzq3aedtYA3c1cg5GmyPYUkw MTAhMAkGBSsOAwIaBQAEFPIcEwgfkB4AhluSzafY7rmeYdvZBAg6hBvCdPUzoQIC CAA= -----END PKCS12-----
失効	失効済み
失効日時	2011/09/21 11:54:43
失効理由	revoked

図 2.6.2-5　デバイス詳細画面（証明書）

表 2.6.2-5　デバイス詳細画面（証明書）項目説明

項目	説明
証明書プロファイルデータ	証明書サブジェクト名のフォーマット、有効期間、証明書拡張など、証明書のフォーマットを定義するデータです。
証明書データ(X509 PEM)	X.509 証明書ファイルの内容
証明書データ(PKCS#12 PEM)	PKCS#12 ファイルの内容
失効	失効している場合、「失効済み」と表示されます。失効していない場合は表示されません。
失効日時	証明書失効日時が表示されます。失効していない場合は表示されません。
失効理由	証明書失効理由（現状は「unspecified」固定です）が表示されます。失効していない場合は表示されません。

2.6.2.6.　　機能説明（デバイス詳細/プロファイル）

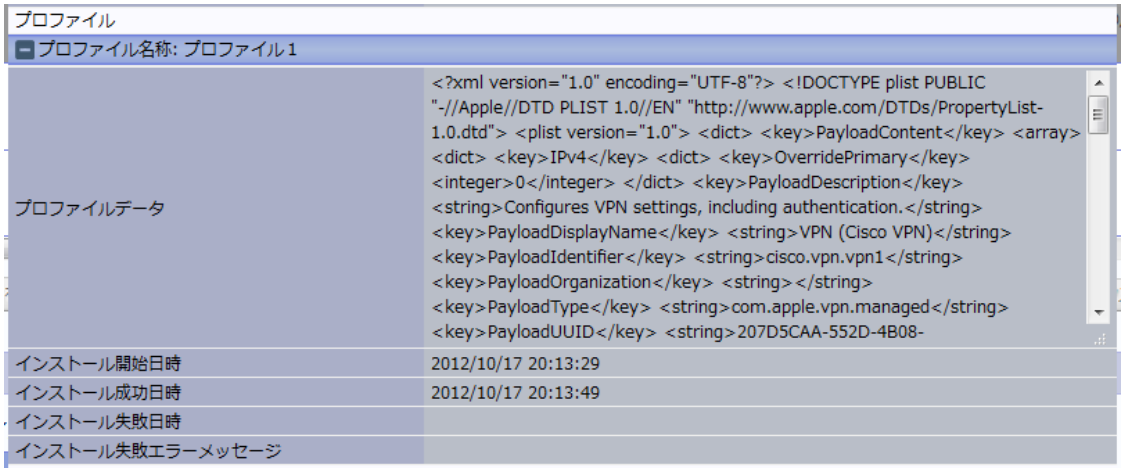


図 2.6.2-6　デバイス詳細画面（プロファイル）

表 2.6.2-6　デバイス詳細画面（プロファイル）項目説明

項目	説明
プロファイルデータ	デバイスに配信する構成プロファイルデータです。
インストール開始日時	構成プロファイルのインストールを開始した時刻です。
インストール成功日時	構成プロファイルのインストールに成功した時刻です。
インストール失敗日時	構成プロファイルのインストールに失敗した時刻です。
インストール失敗エラーメッセージ	構成プロファイルのインストールに失敗したエラーメッセージが表示されます。

2.6.2.7. 機能説明（スキーマ管理）

本サービスでは利用しません。

2.6.2.8. 機能説明（グループ管理）

本サービスでは利用しません。

2.6.2.9. 機能説明（プロファイル管理）

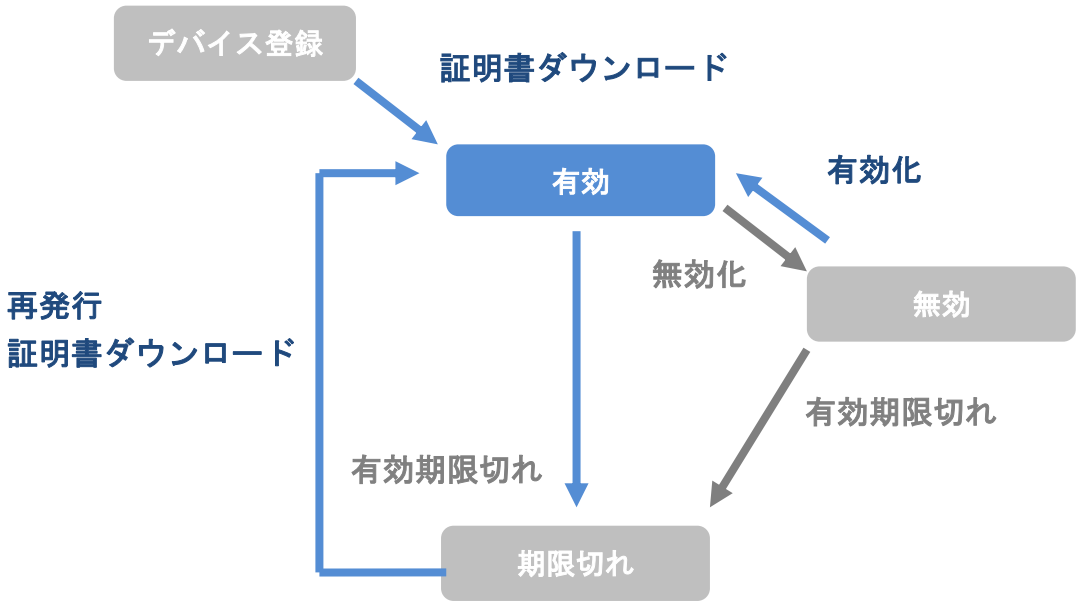
本サービスでは、プロファイル管理はご利用できません。

3. X-pointの利用準備を行う

3.1. 証明書発行の基本

3.1.1. クライアント証明書のライフサイクル

本サービスで利用するクライアント証明書は、以下のようなライフサイクルで運用されます。



証明書の状態	説明
デバイス登録	証明書を発行する前の状態です。この時点でライセンス数にカウントされます。
有効	ご利用端末から証明書をダウンロードすると証明書が有効に利用できる状態になります。 同一デバイスで複数の証明書を発行してもライセンスとしてカウントされません。
無効	管理者により証明書の利用が禁止された状態です。 CRL(失効リスト)更新タイミングで本証明書を利用することができなくなります。 また、有効化で証明書が利用可能となります。
期限切れ	証明書に記載された有効期限が過ぎて失効した状態です。 本証明書を利用することはできません。

3.1.2. 証明書発行管理業務

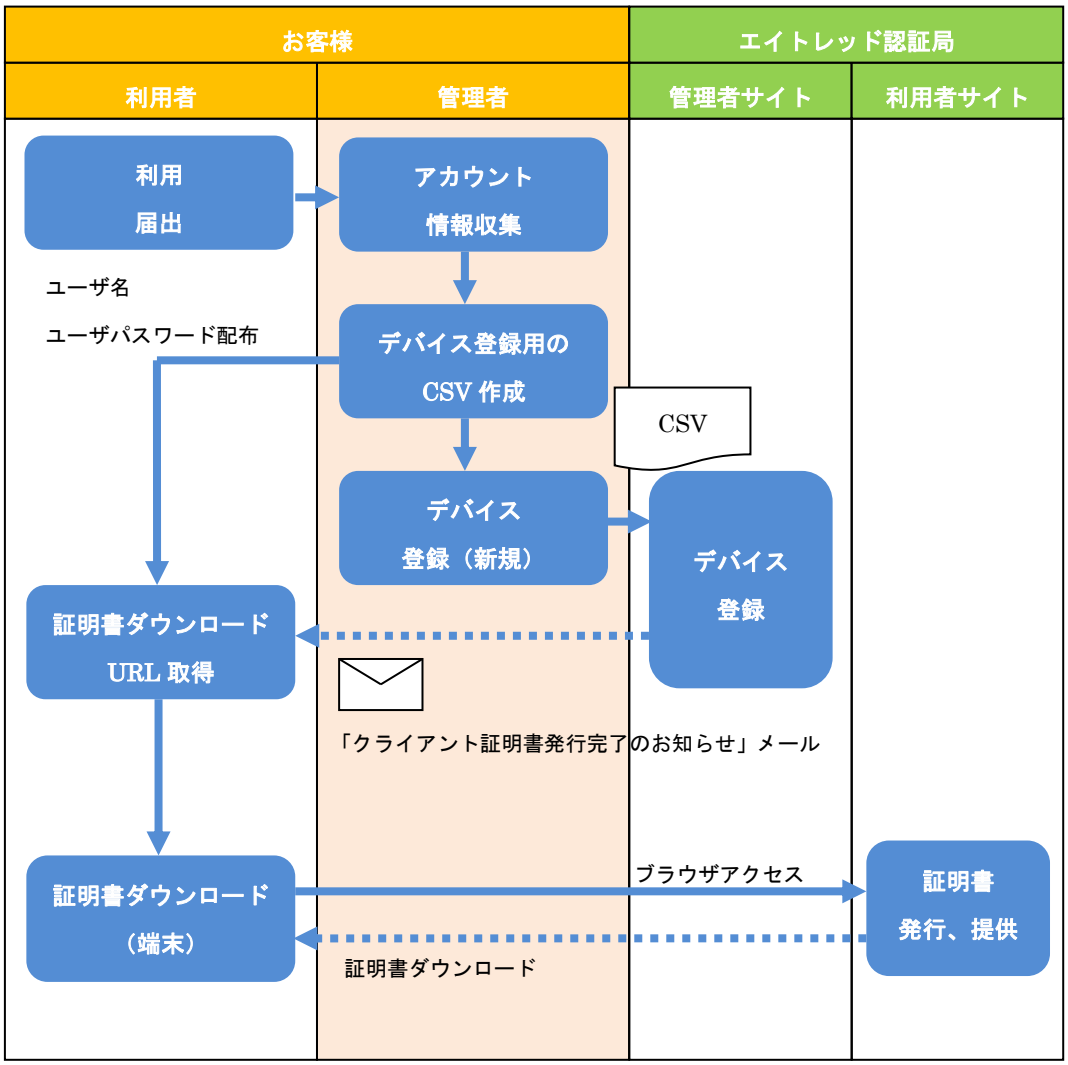
クライアント証明書の発行管理を行うための主な業務は以下の通りです。

業務	業務概要	参照
デバイス登録	社外で X-point サービスを利用するデバイスを登録する業務です。 デバイス毎の証明書ダウンロード用 URL にアクセスすることでクライアント証明書が発行されます。	「3.2 X-point 利用者の証明書を発行する」
証明書再発行	既に発行済みのクライアント証明書の期間を更新して発行するための業務です。	「3.3 X-point 利用者の証明書を更新する」
証明書無効	既に発行済みのクライアント証明書を無効化するための業務です。 例えば、利用者がデバイスを紛失したためアクセスを無効化したい、管理者の判断により利用者のデバイスからのアクセスを無効化したい、などのケースが想定されます。	「3.4 X-point 利用者がデバイスを紛失したら」
デバイス削除	社外で X-point サービスを利用するデバイスを削除する業務です。 例えば、退職や転属などで X-point Cloud を利用しなくなる場合などのケースが想定されます。	「3.5 X-point の利用デバイスが不要になったら」

3.1.3. 証明書発行管理業務の流れ

前述の証明書発行業務についてそれぞれ業務の大きな流れをご説明いたします。

【証明書発行までの流れ(デバイス登録)】



1) お客様管理者は利用者の情報(氏名、メールアドレス等)を収集し、スキーマ設定に合わせたデバイス登録用の CSV を作成します。

2) 証明書をダウンロードするサイトにログインするために管理者が取り決めたユーザ名、パスワードを各利用者宛に通知してください。

3) エイトレッド認証局に作成したデバイス登録用の CSV でデバイス情報を登録します。(※1)

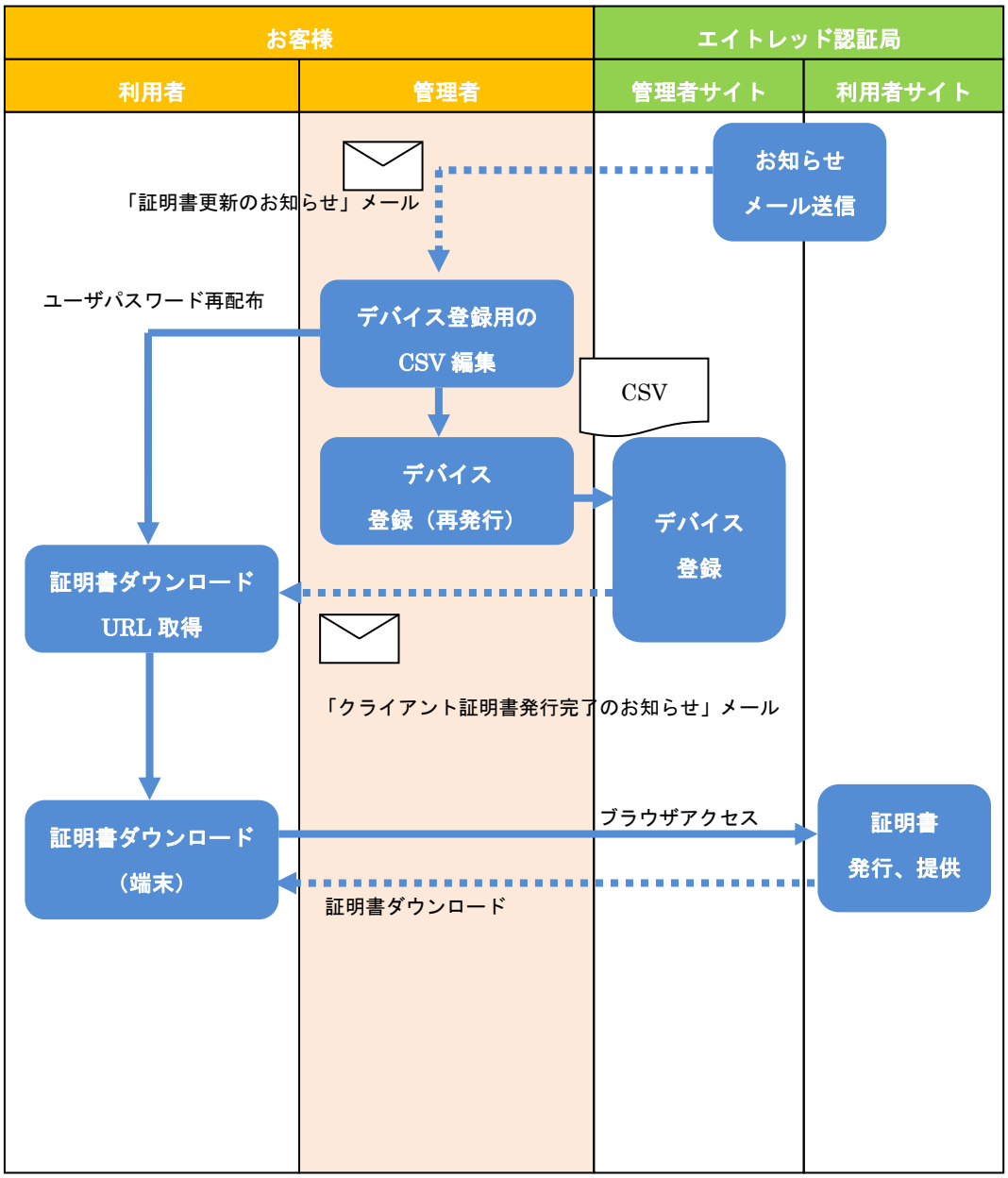
4) エイトレッド認証局は利用者に証明書ダウンロード用の URL が記載されたメールを送信します。(※2)

5) 利用者はダウンロード URL にアクセスし、ユーザ名、ユーザパスワードを入力し、証明書をインストールします。

※1 発行の種類で「新規発行」を選択します

※2 利用者にメール通知するためにはスキーマ設定で「メールアドレス」、グループ設定で「URL 通知」が選択されている必要があります。尚、メール通知しない場合は、管理者サイトにてデバイス毎のダウンロードURL を確認することができます。

【証明書更新までの流れ(証明書再発行)】



1) エイトレッド認証局から証明書の有効期限 60 日前に「証明書更新のお知らせメール」が届きます。
※事前通知の期間 60 日は変更できません。

2) 再発行時に証明書ダウンロード用のユーザパスワードを変更する場合は、新規登録時に作成した CSV を編集します。
（更新を行わないユーザ情報は削除してください）

3) ユーザパスワードを変更した場合は、利用者毎に CSV に設定したユーザパスワードを再配布します。

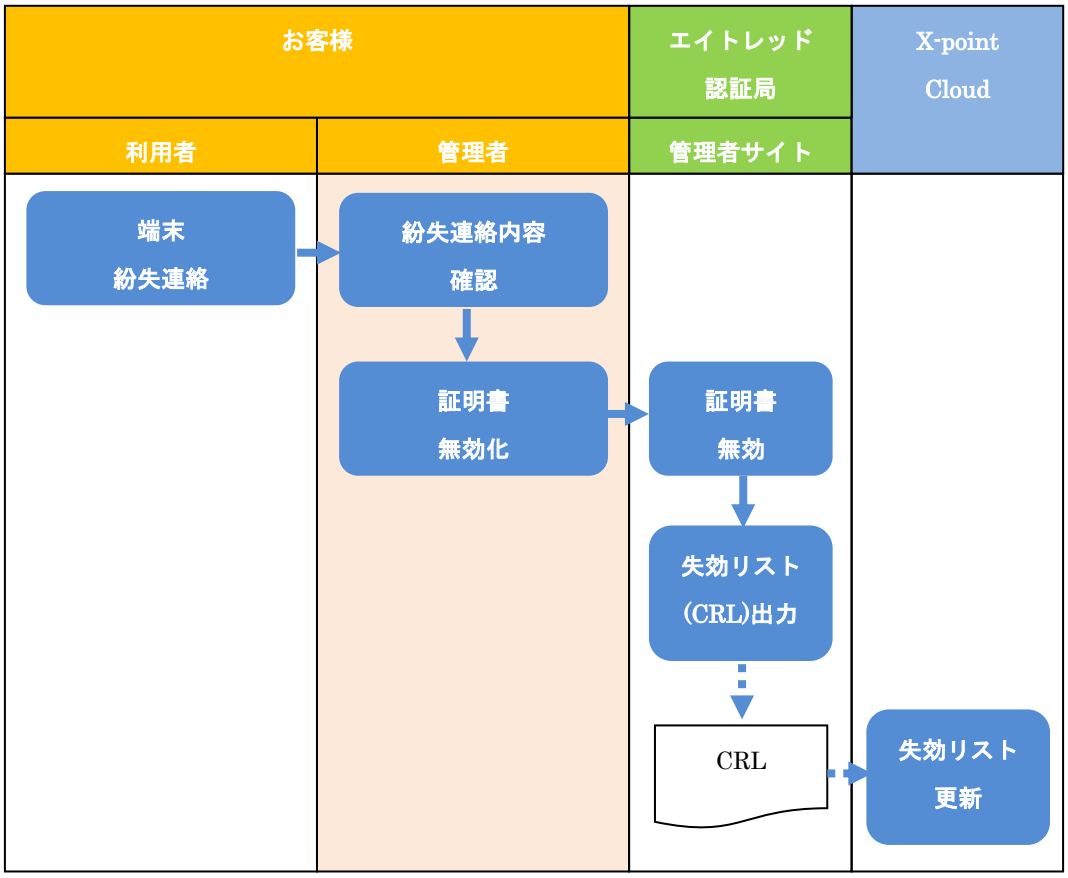
4) エイトレッド認証局に作成したデバイス登録用の CSV でデバイス情報を登録します。
（※1）

5) エイトレッド認証局は利用者に証明書ダウンロード用の URL が記載されたメールを送信します。

6) 利用者はダウンロード URL にアクセスし、ユーザ名、ユーザパスワードを入力し、証明書を再インストールします。

※1 発行の種類で「再発行」を選択します

【証明書無効化までの流れ(証明書無効)】



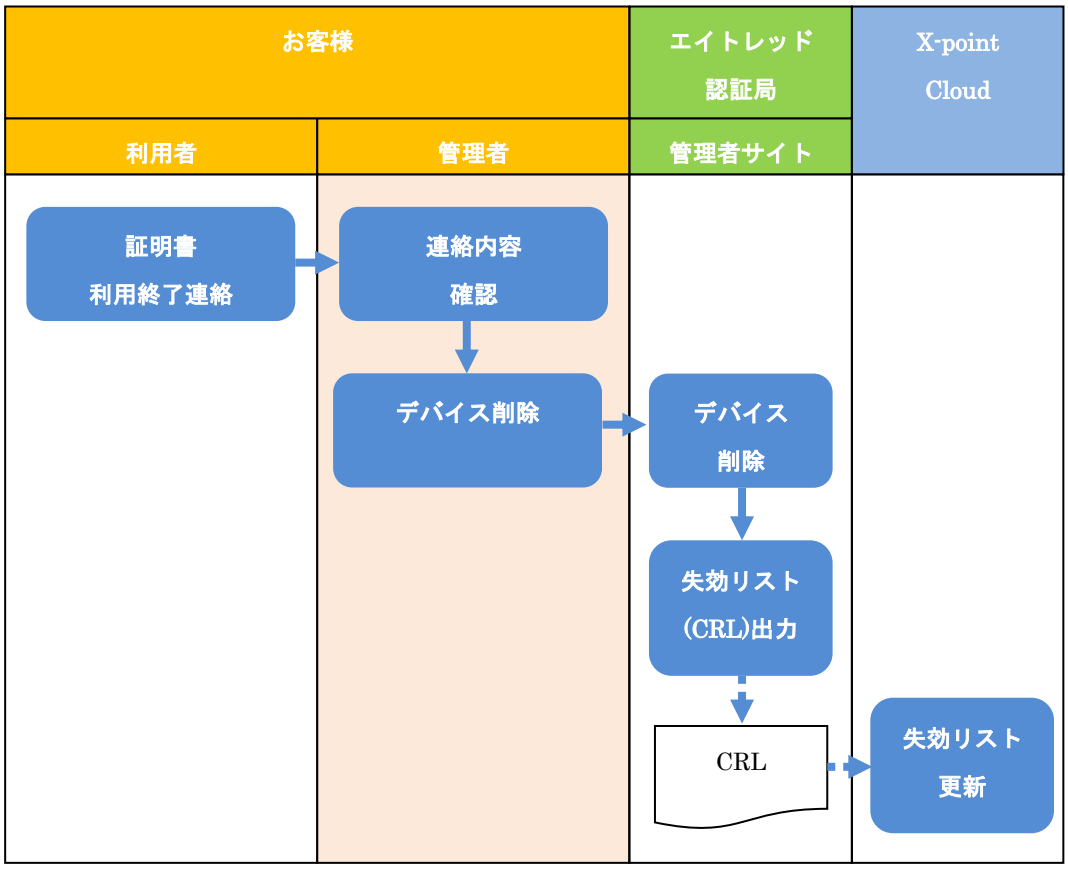
1) お客様利用者は端末の紛失連絡を管理者に行います。

2) お客様管理者は証明書の無効化処理を行います。

3) X-point Cloud は夜間に失効リストの更新を行います。
リストが更新されると該当の証明書でX-pointにアクセスすることができなくなります。

4) お客様利用者の必要に応じて、証明書を再発行します。

【証明書削除までの流れ(証明書削除)】



1) お客様利用者は利用終了の連絡を管理者に行います。

2) お客様管理者はデバイスの削除処理を行います。

3) X-point Cloud は夜間に失効リストの更新を行います。
リストが更新されると該当の証明書でX-pointにアクセスすることができなくなります。

3.1.4. 証明書ライセンスのカウント

お客様の証明書発行業務運用における証明書ライセンス数は登録されたデバイス数に依存します。ライセンス数のカウント方法は以下のとおりです。

- デバイス情報を１つ登録することで１カウントされます（発行可能数が１減ります）
- デバイス情報を１つ削除することで１カウントダウンされます（発行可能数が１増えます）

なお、契約端末数および登録端末数は「デバイス管理画面」の左上（契約端末数／登録端末数）に表示されています。

3.2. X-point 利用者の証明書を発行する

本節では、X-point 利用者用のクライアント証明書を発行するまでの手順をご説明いたします。

クライアント証明書を利用するには、エイトレッド認証局にてデバイスを登録する必要があります。

3.2.1. デバイス登録用の CSV を準備する

メモ帳などのテキストエディタ、または Microsoft Office Excel で、以下の項目順に CSV を作成します。

・ユーザ名

・ユーザパスワード

・メールアドレス

■各項目の入力制限事項

項目名	必須	最大データ長	使用可能文字	フォーマット
ユーザ名	○	64Byte	・他のユーザ名と重複しない任意の文字列 ・半角英字(a ～z、A～Z) 、半角数字(0 ～9) 、スペース、カンマ(,) 、ピリオド(.)、ハイフン(-)、スラッシュ (/)、丸括弧 (())、プラス符号 (+)、等号 (=) 、シングルクォーテーション(') 、アンダースコア(_)	下記は不可 ・半角スペースのみ ・文字列前後に半角スペース
ユーザパスワード	○	80Byte	・半角英字(a ～z、A～Z) 、半角数字(0 ～9) 、カンマ(,) 、ピリオド(.)、ハイフン(-)、スラッシュ (/)、丸括弧 (())、プラス符号 (+)、等号 (=) 、シングルクォーテーション(') 、アンダースコア(_)	
メールアドレス	○	128Byte	・半角英字(a ～z、A～Z) 、半角数字(0 ～9) 、アットマーク(@) 、カンマ(,) 、ピリオド(.)、ハイフン(-)、スラッシュ (/)、丸括弧 (())、プラス符号 (+)、等号 (=) 、シングルクォーテーション(') 、アンダースコア(_)	

■CSV フォーマット制限事項

1. 各項目間の区切り文字はカンマ(,)区切りとする。
2. 項目にカンマが含まれる値を使用する場合は、値の前後をダブルクォート(“)で囲ってください。
3. ファイルの拡張子は「.csv」にしてください。
4. ファイルの文字コードは「Shift-JIS」、改行コードは「CRLF」にしてください。
5. 一度に登録できるデバイス情報の上限は 500 件となります。

作成例）

ファイル名：sample01.csv

```
atled01,atled01_pass,atled01@atled.jp      ⇒  A
atled02,atled02_pass,atled02@atled.jp      ⇒  B
atled03,atled03_pass,atled03@atled.jp      ⇒  C
・・・
```

＜説明＞

A

「atled01」：証明書ダウンロード用ユーザ名

「atled01_pass」： 証明書ダウンロード用パスワード

「atled01@atled.jp」：証明書ダウンロード用 URL の通知先（email）

B

「atled02」：証明書ダウンロード用ユーザ名

「atled02_pass」： 証明書ダウンロード用パスワード

「atled02@atled.jp」：証明書ダウンロード用 URL の通知先（email）

C

「atled03」：証明書ダウンロード用ユーザ名

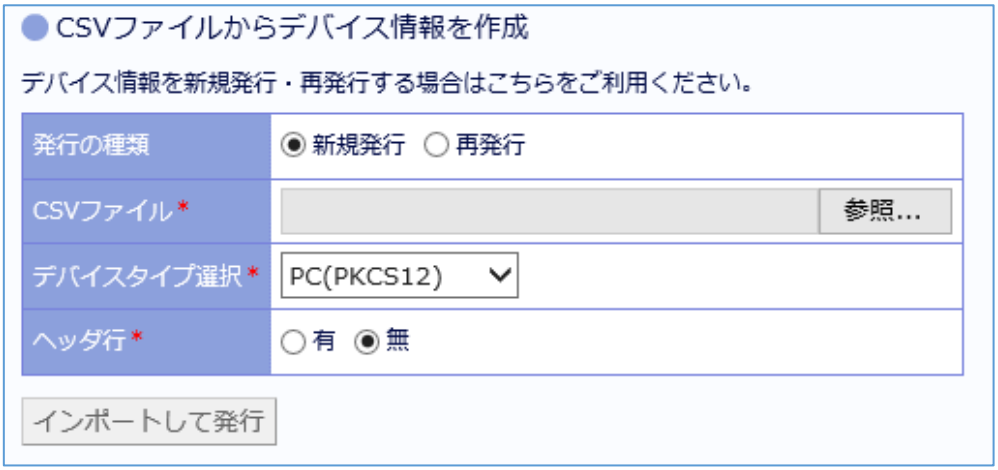
「atled03_pass」： 証明書ダウンロード用パスワード

「atled03@atled.jp」：証明書ダウンロード用 URL の通知先（email）

3.2.2. デバイス情報を登録する

1) 管理者サイトにログインします。

2) ログイン後の画面「デバイス管理」下部にデバイス情報を登録する画面があります。



3) 発行の種類に「新規発行」が選択されていることを確認します。

4) 「参照」ボタンを押下して作成した CSV ファイルを選択します。

5) デバイタイプを選択します。

デバイスタイプが違う場合、デバイスタイプ毎にインポートする必要があります。

利用環境	ブラウザ／ツール	デバイスタイプ
Windows	Google Chrome Microsoft Edge(Chromium 版) Mozilla Firefox eFormMaker	PC(PKCS12)
Mac	Apple Safari	
Android	Chrome for Android	
iOS	Mobile Safari	PKCS12(Email)

※デバイスタイプに「PKCS12(Email)」を選択している場合は、デバイスで受信できるメールアドレスを指定してください。

6) 「ヘッダ行」は「無」を選択します。

7) 「インポート」ボタンを押下します。

インポートすると同時に利用者にはクライアント証明書発行に関するご案内メールが送信されます。

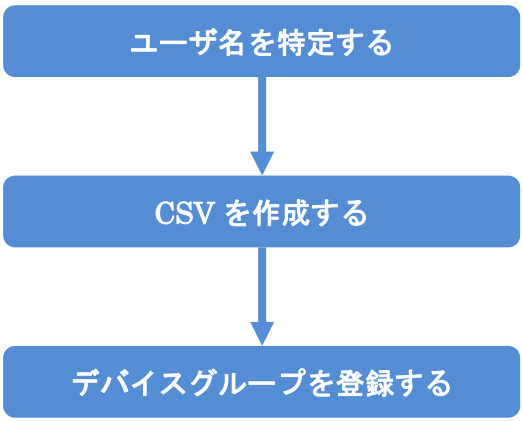
8) デバイス一覧にデバイス情報が登録されたことを確認します。

3.3. X-point 利用者の証明書を更新する

本節ではクライアント証明書を更新または追加発行する手順をご説明いたします。

クライアント証明書を更新または追加発行するケースとしては以下のようなものが想定されます。

- 利用者の証明書の有効期限が切れた
- インストールした証明書を誤って削除してしまった



再発行するユーザのユーザ名を特定します。

再発行するユーザのみの CSV ファイルを作成します

※ユーザ名を変更することはできません。

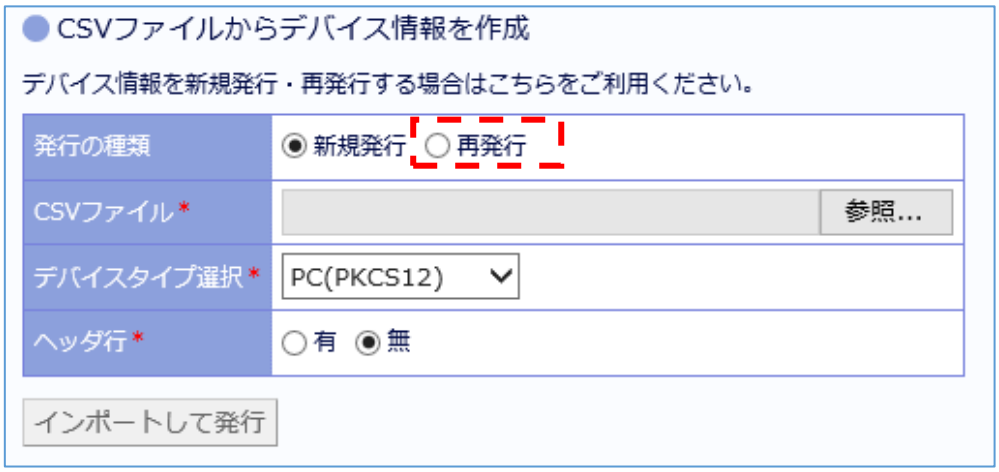
管理サイトから作成 CSV でデバイス情報を登録します。

※CSV をインポートする際に、発行の種類に「再発行」を選択してください。

3.3.1. クライアント証明書を再発行（更新）する。

クライアント証明書を再発行（更新）する場合も、「3.2 X-point 利用者の証明書を発行する」を参照してデバイス登録用の CSV を準備してから、デバイス登録を行ってください。

デバイス登録する際には発行の種類で「再発行」を選びます。

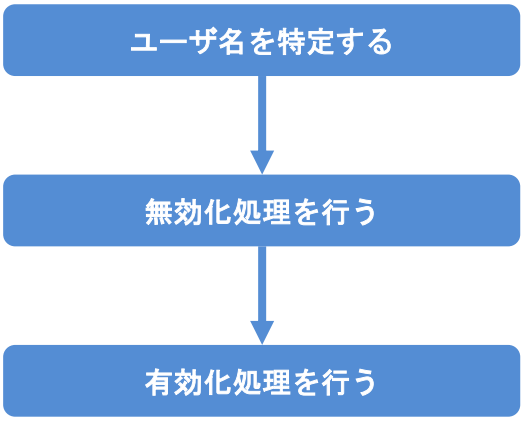


3.4. X-point 利用者がデバイスを紛失したら

本節ではクライアント証明書を一時的に無効する手順をご説明いたします。

クライアント証明書を無効化させるケースとしては以下のようなものが想定されます。

- 利用者がデバイスを紛失したためアクセスを無効化したい
- 管理者の判断により利用者のデバイスからのアクセスを無効化したい



失効させるユーザ名を特定します。

証明書一時的に無効化させます。

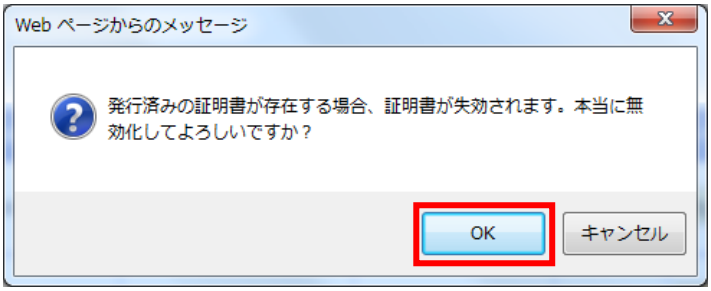
一時的に無効化した証明書を有効にします。

■無効化処理を行う

1) エイトレッド認証局にログインします。

①デバイス一覧から対象ユーザの「無効化」ボタンをクリックします。

②メッセージを確認して、「OK」をクリックします。

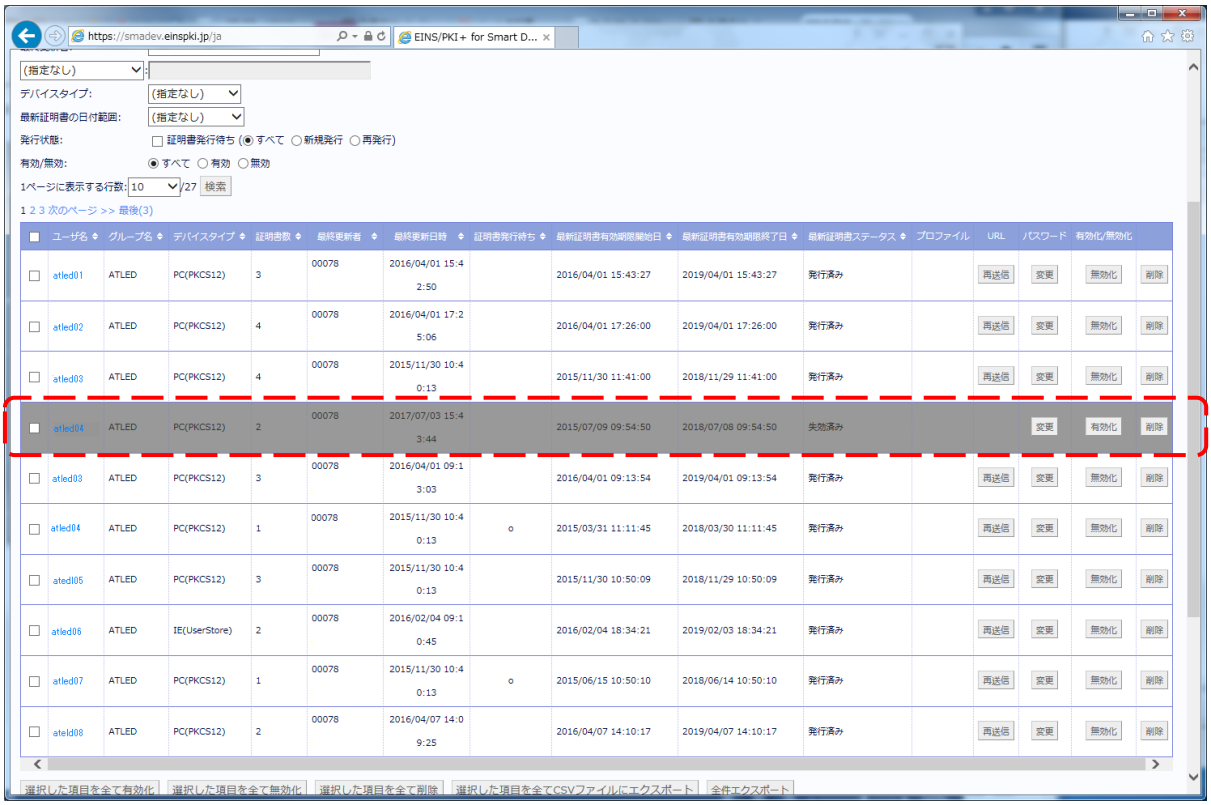


！注意事項

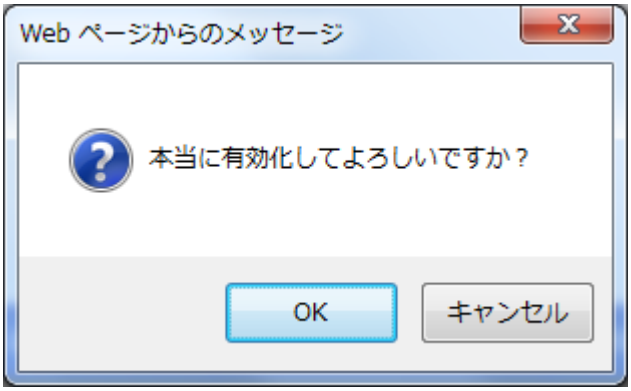
無効化した場合「有効化」により証明書が再度利用できるようになりますが、CRL(失効リスト)に有効化したことが反映されるまではX-pointにアクセスすることは出来ません。

■有効化処理を行う

①　デバイス一覧から対象ユーザの「有効化」ボタンをクリックします。



②メッセージを確認して、「OK」をクリックします。

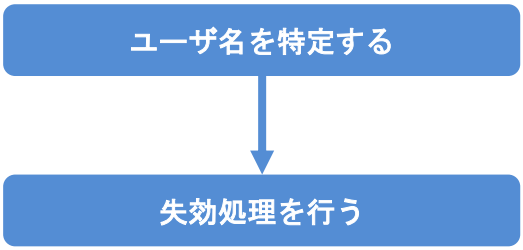


3.5. X-point の利用デバイスが不要になったら

本節では利用者情報を含めてクライアント証明書を削除する手順をご説明いたします。

利用者情報を含めてクライアント証明書を削除するケースとしては以下のようなものが想定されます。

- 退職・異動などで利用者が今後、証明書を使うことがなくなった



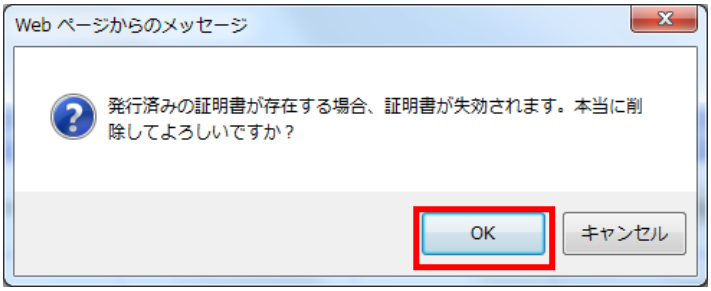
失効させるユーザ名を特定します。

証明書を失効させます。

1)エイトレッド認証局にログインします。

①デバイス一覧から対象ユーザ「削除」ボタンをクリックします。

②メッセージを確認して、「OK」をクリックします。

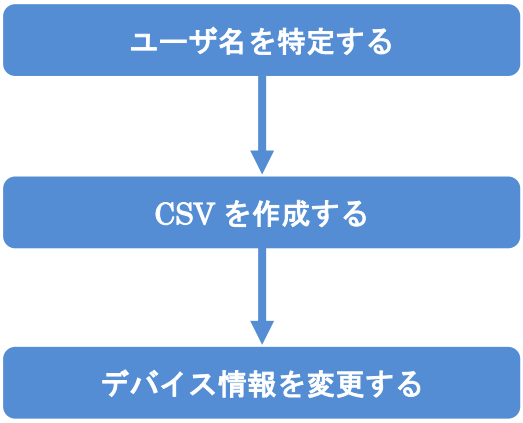


！注意事項

無効化した場合「有効化」により証明書が再度利用できるようになりますが、削除の場合デバイス情報自体が削除させるため証明書の再利用することはできません。

3.6. 一括でデバイスの有効化・無効化・削除を行う

本節では前項で説明したデバイスの有効化・無効化・削除を一括で行う手順ををご説明いたします。



有効化・無効化・削除するユーザのユーザ名とそのユーザのデバイスタイプを特定します。

有効化・無効化・削除を行うユーザのみの CSV ファイルを作成します。

管理サイトから作成 CSV でデバイス情報を変更（有効化、無効化、削除のいづれかを選択）します。

3.6.1. CSV ファイルを作成する。

メモ帳などのテキストエディタ、または Microsoft Office Excel で、以下の項目順に CSV を作成します。
CSV のフォーマットは下記となります。

（1 行目：ヘッダ行）「ユーザ名」固定

（2 行目以降：データ行）デバイスの有効化、無効化、削除を行うデバイスのユーザ名

となります。

■CSV フォーマット制限事項

1. 各項目間の区切り文字はカンマ(,)区切りとする。
2. 項目にカンマが含まれる値を使用する場合は、値の前後をダブルクォート(“)で囲ってください。
3. ファイルの拡張子は「.csv」にしてください。
4. ファイルの文字コードは「Shift-JIS」、改行コードは「CRLF」にしてください。

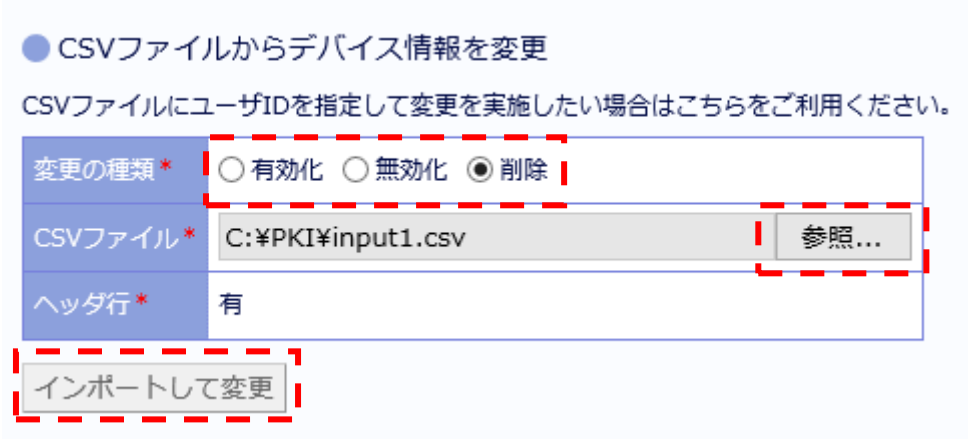
■CSV ファイル作成例

```
ユーザ名
user01
user02
```

3.6.2. デバイスの有効化・無効化・削除を行う。

1) 管理者サイトにログインします。

2) ログイン後の画面「デバイス管理」下部にデバイス情報を変更する画面があります。

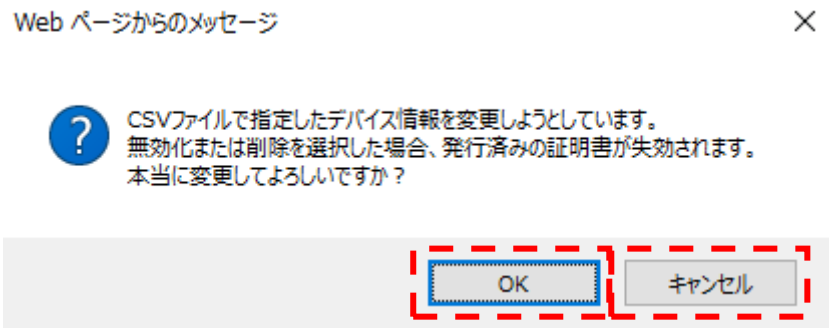


3) 変更の種類から「有効化」、「無効化」、「削除」を選択します。

4) 「参照」ボタンを押下して作成した CSV ファイルを選択します。

5) 「インポート」ボタンを押下します。

6) 確認画面が表示されますので、変更する場合は「OK」ボタン、変更しない場合は「キャンセル」ボタンをクリックします。



4. Q＆A

4.1. クライアント（デバイス）証明書は、どのように発行されるのでしょうか？

ユーザが証明書ダウンロード用の URL にアクセスして、証明書をダウンロードする際に発行されます。

4.2. 証明書発行 URL 通知にユーザ名、パスワードを付与して送信できますか？

発行時に送付されるメールにユーザ名およびパスワードを付与して送信することはできません。

4.3. 間違った CSV で新規発行をしてしまった場合、どう対応するのが適切でしょうか？

■発生するケースは以下の場合が考えられます。

・違う人のメールアドレスでデバイス登録してしまった。

■対応方法

以下のような対処方法があります。

1. デバイス管理画面にログインし、誤って新規発行してしまったデバイス情報の「無効化」を行う。
   （画面右に無効化ボタンがあります）
2. 誤った証明書をインポートした端末から、証明書が使用できないことを確認し、証明書の削除を行う。

   ！注意事項

   「無効化」したデバイスは、翌日 2:00 に証明書失効リストに反映されますので、それまでは使用できます。
3. デバイス管理画面から、先ほど「無効化」したデバイス情報を削除する。
4. CSV ファイルに正しい内容を記載して新規発行を行う。

4.4. 証明書を「無効」にできますが、これはどういったシーンで利用するものでしょうか。

デバイス管理画面にデバイス情報を残したまま証明書を失効したい場合に、「無効化」を実施します。
例えば、すでに証明書が発行済みの利用者様が PC をリプレイスする場合、管理コンソール上からデバイス情報を「無効」化しておき、証明書を一度失効させます。その後、新 PC 上で証明書インストールの準備が整ったら、管理コンソール上からデバイス情報を「有効」化し、新 PC に旧 PC と同じ ID・PW で証明書を発行することができます。
なお、無効化しても契約端末数としては引き続きカウントされます。

4.5. 証明書有効期限終了日を全ユーザー一律に合わせることは可能でしょうか？

証明書の有効期限終了日は、利用者が証明書発行処理を実施してから 365 日後、となりますので、有効期限終了日を全ユーザー一律で合わせることはできません。

4.6. 証明書を無効にした場合、いつごろ証明書が使えなくなるのでしょうか。

証明書を失効した場合、翌日 2:00 に証明書失効リストに失効された証明書情報が反映されます。
それまでは失効した証明書の利用が可能です。

4.7. エイトレッド認証局でデバイス削除すると利用者側で現行の証明書は表示されなくなりますか？

エイトレッド認証局でデバイスを削除しても、利用者側デバイスには証明書は表示されますが、証明書認証には利用できなくなります。不要な証明書は利用者側デバイスで削除することをお勧めします。

4.8. エイトレッド認証局のログイン証明書をインストールする際にインストールエラーになります。

PC の時間が現在時刻とずれている可能性があります。
PC の時間を現在時刻に修正していただき、該当ユーザのログイン証明書を再発行してください。

4.9. 証明書発行上限に達した場合はどうするのでしょうか？

発行した証明書単位で削除することはできません。証明書を削除するには、一度デバイス情報を削除して頂く必要がございます。

4.10. デバイス管理画面で CSV ファイルを使わずにデバイス情報を登録できますか？

デバイス管理画面上で CSV ファイルを使わずにデバイス情報を登録することはできません。
デバイス情報を登録する方法は CSV ファイルのインポートのみに対応しております。

4.11. iPhone のブラウザでのみクライアント証明書を利用していて、途中からスマートアプリでクライアント証明書を利用したい場合。

iPhone のクライアント証明書を削除し、対象端末のデバイス削除後に「デバイスタイプに「PKCS12(Email)」で新規デバイス登録を行ってください。

新規デバイス登録後、iPhone のブラウザとスマートアプリにクライアント証明書をインストールしてください。

5. 困ったときは

下記の場合、「X-point サポート」までお問い合わせください。

・エイトレッド認証局のログイン ID、ログインパスワードを忘れた。

・管理者のメールアドレスを変更したい。

・管理者が変わったため、管理者用のログイン証明書を再発行してほしい。

・管理者用のログイン証明書の有効期限が切れた。

・デバイス数を変更したい。

・その他、マニュアルに記載されていない事項など。

■改訂履歴

改版	改版内容
2021 年 4 月 1 日版	初版リリース
2022 年 1 月 12 日版	1.1　対応環境 ・対応ブラウザに「Edge、Chrome」を追加 1.2.　　Microsoft Internet Explorer の「インターネットオプション」設定 ・削除 2.4. 前提条件・制限事項等 ・X-point Cloud 動作環境のリンク先を変更 3.2.2.　デバイス情報を登録する ・利用環境文章を削除し。新たに対応表を挿入。
2022 年 2 月 1 日版	1.1　対応環境 ・OS に「Windows11」を追加
2022 年 8 月 24 日版	はじめに ・対応バージョンからマイナーバージョン部を削除（v3.0 → v3） 全般 ・下記から「Internet Explorer」の表記を削除 商標について 1.1　対応環境 1.3　本書における用語説明 3.2.2 デバイス情報を登録する 4.2 「Internet Explorer ではこのページは表示できません。」というメッセージが 表示されてしまいます。 4.11 SharePoint にアクセスすると何度もクライアント証明書を要求されます。
2024 年 8 月 26 日版	2.4.4. 各サービスとの併用 ・「サイボウズリモートサービス（有償オプション）」を削除。 3.2.1. デバイス登録用の CSV を準備する ・使用可能文字の誤記を修正。 ・メールアドレスの使用可能文字にアットマーク(@)を追加
2025 年 11 月 18 日版	1.1　対応環境 ・OS から「Windows7,8.1」を削除 2.2.　　クライアント証明書サービス仕様 ・ダイジェストアルゴリズムを「SHA-256」に変更