管理番号 CSI2020-0708

代理認証システム
マニュアル
（機関向け）

東北大学
サイバーサイエンスセンター
CSI 研究室

版	作成年月日	承認	査閲	作成	備考(改版理由他)
1.0	2008/12/03			大和	
1.1	2020/07/08			後藤	ユーザインタフェース更新

目次

第1章　はじめに

本書は、eduroam 代理認証システム(以下、代理認証システム)の機関向けの操作法を記述したものです。
代理認証システムを使用するには、eduroam JP 事務局を通じて、事前に機関管理者の登録が必要です。

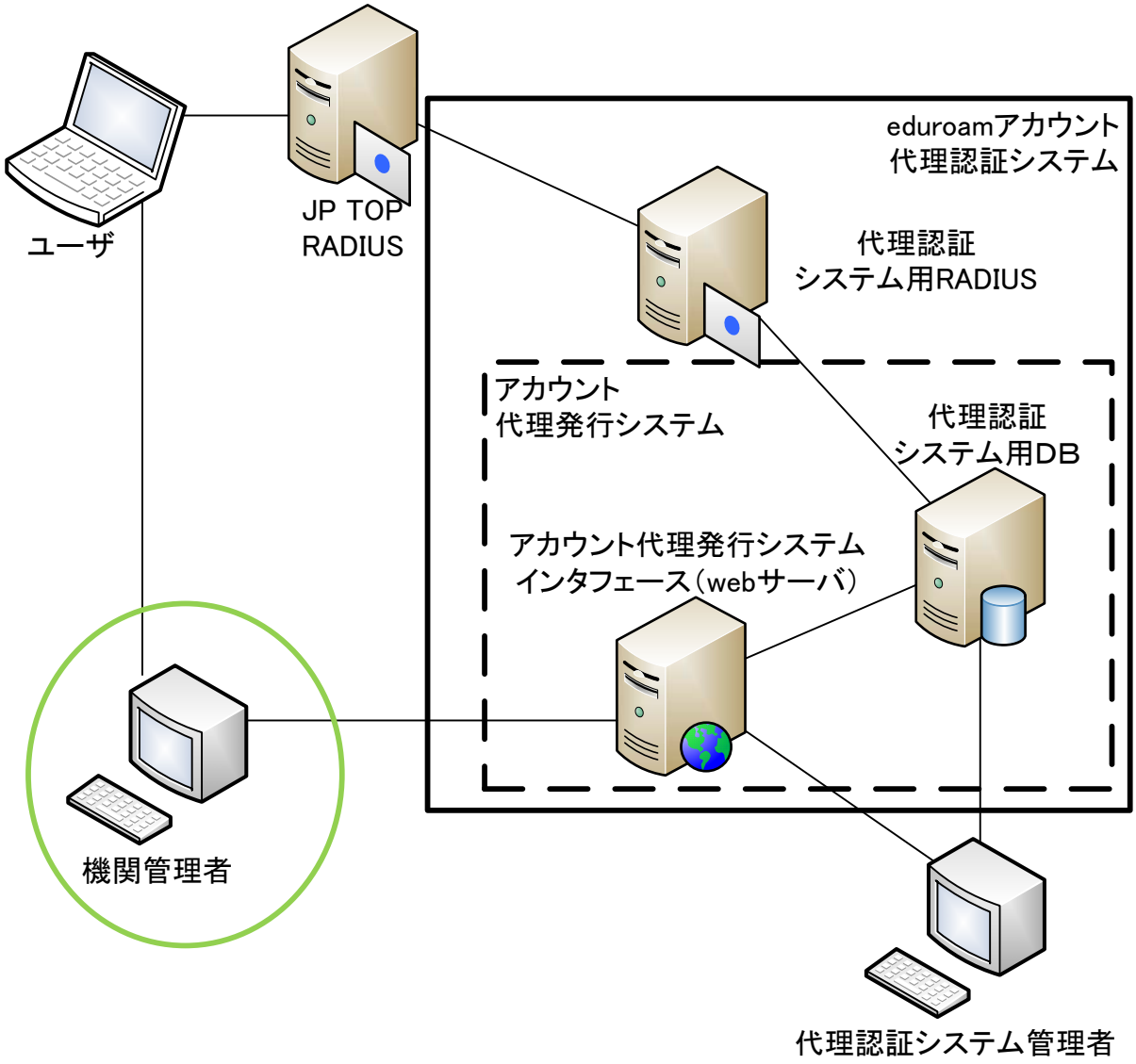

図 1 代理認証システムの構成

1.1 用語の説明

- アカウント: eduroam の認証に使用するユーザ名

第2章　使用方法

2.1 アクセス手順

1. https://tanelon3.rd.cc.tohoku.ac.jp/deas/inst/ にアクセスする。
2. メニューから操作を選択する。
   - ユーザ名(ID)とパスワードを入力するボックスが表示されます。
   - 代理認証システムに登録されている機関管理者の ID とパスワードを入力してください。

2.2 操作一覧

機関で行える操作には、eduroam 用のアカウントの発行等を行うアカウント管理と、機関管理者の追加等を行う機関管理があります(図 2)。

それぞれ下記の操作が行えます。操作は次章以降で説明します。

- アカウント管理（第 3 章）
  - アカウント一覧／パスワード一覧ダウンロード（3.2）
    - 発行済みアカウントの一覧表示
    - 発行済みアカウントのパスワード込みの情報を、CSV 形式でダウンロード
  - アカウント追加（3.3）
    - アカウントの発行
  - アカウントロック／解除（3.4）
    - アカウントの使用禁止および解除
  - 利用者パスワード変更（3.5）
    - 利用者パスワードの変更
- 機関管理（第 4 章）
  - 機関管理者一覧（4.1）
    - 登録されている機関管理者の一覧表示
  - 管理者追加（4.2）
    - 機関管理者の追加
  - 管理者のロック／解除（4.3）
    - 機関管理者の使用禁止および使用禁止の解除
  - 自パスワード変更（4.4）
    - 自分の ID のパスワード変更
  - パスワード変更（4.5）
    - 自機関の機関管理者に新しいパスワードを設定

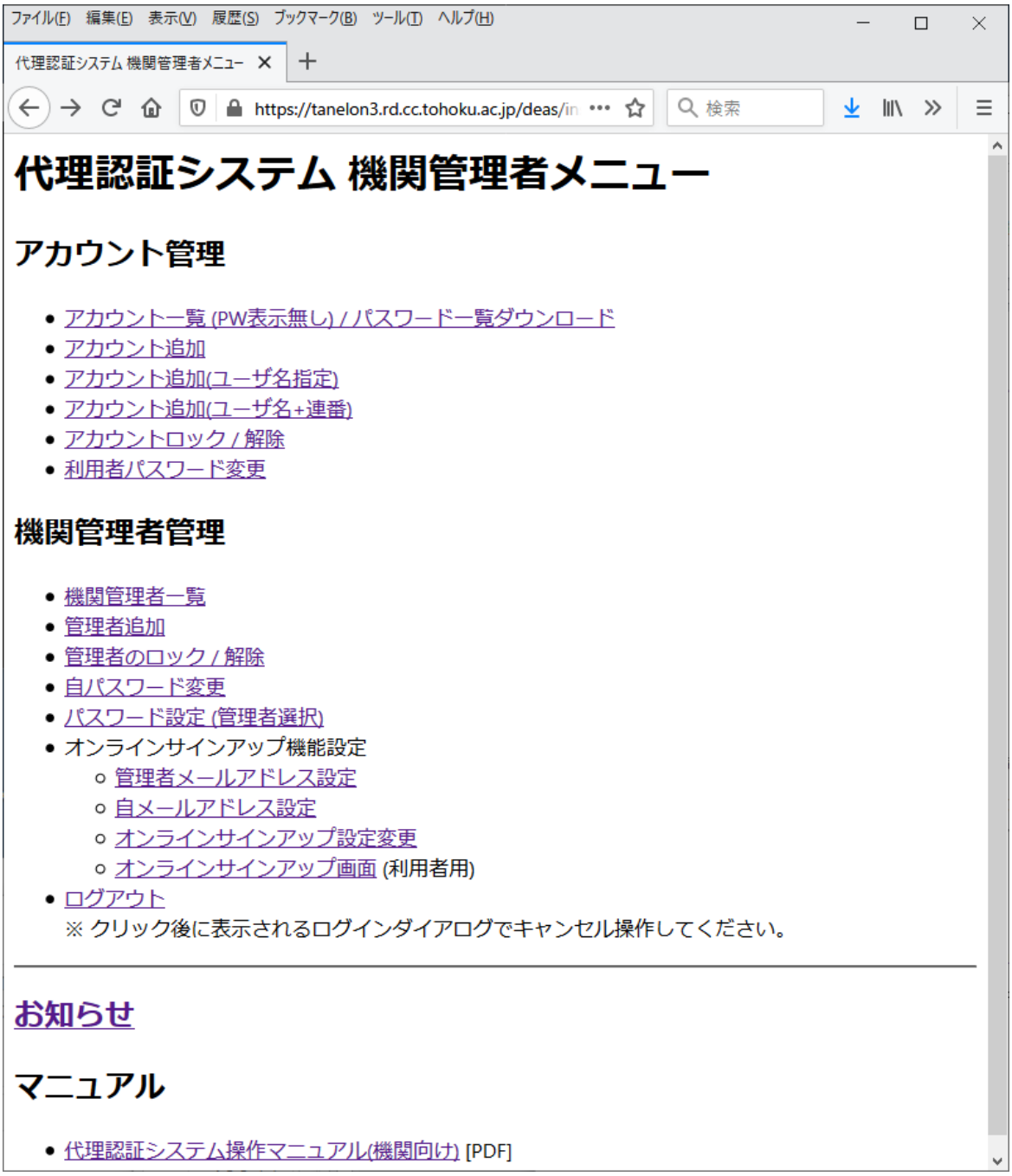

図 2 代理認証システム 機関管理者メニュー (例)

第3章　アカウント管理

この章ではアカウント管理の各操作を説明します。
対象となるアカウントは自機関で登録したアカウントです。

3.1　有効なアカウント

代理認証システムでは、利用者がアカウントとパスワードを正しく入力しても、下記の全てが整わないとネットワークアクセスが許可されません。

- 使用期間内であること
- 代理認証システム管理者が使用を禁止していないこと
- 機関管理者が使用を禁止していないこと

※ IEEE802.1X 方式の制約により、通常、アクセスポイントから端末に対して、どの要因でアクセスが失敗したかは通知されません。

3.2　アカウント一覧／パスワード一覧ダウンロード

発行済みのアカウントが登録の逆順に表示されます(画面にパスワード表示なし)。
発行済みアカウントのパスワード込みの情報を、CSV 形式でダウンロードできます。

3.2.1　列の説明

- id
  - システムが採番した一意識別子
- ユーザ名
  - 払い出されたアカウント名
- 有効
  - 使用期間外および使用禁止により使用できないアカウントは“無効”、使用できるアカウントは“有効”と表示
- センターロック
  - 代理認証システム管理者が使用禁止にしたアカウントは“LOCKED”と表示
- ロック
  - 機関管理者が使用禁止にしたアカウントは“LOCKED”と表示
- 証明書, 証明書シリアル
  - (未実装)
- 使用開始
  - アカウントが有効となる日時のタイムスタンプ
- 使用終了
  - アカウントが無効となる日時のタイムスタンプ

- 登録日
  - アカウントが発行された時点のタイムスタンプ
- start / end
  - パスワード一覧のダウンロード範囲(開始・終了位置)を指定するボタン

3.2.2 パスワード一覧ダウンロード手順

1. アカウント一覧の表示
   - アカウントの一覧が表示されます
2. 出力範囲の決定
   - 出力する範囲を“start”と“end”で指定します。
3. 画面下部にある“download password list”をクリック
4. CSV 形式のファイルが生成され、ダウンロードできます。
   このファイルは Excel 等のアプリケーションで読み込むことができます。

3.2.3 CSV ファイルの形式

CSV ファイルの内容は、下記のように並んでいます。

ID, password, start, end, reg. date

- ID
  - 払い出されたアカウント名 (レルム込み)
- password
  - アカウント用のパスワード
- start
  - eduroam の利用が有効になる日時のタイムスタンプ
- end
  - eduroam の利用が無効になる日時のタイムスタンプ
- reg. date
  - アカウント登録時点のタイムスタンプ

3.3 アカウント追加

アカウント発行に使用します。

3.3.1 手順

1. 発行関連のパラメータを入力
2. “send”をクリック
3. 発行されたアカウントのアカウント名とパスワードが表示される
4. “download”をクリックすることで、CSV 形式で発行アカウントの情報をダウンロードできる

- CSV ファイルの内容は3.2.3参照

3.3.2 入力

アカウント発行時には下記を指定してください。

- 使用開始日
  - 利用者が eduroam の使用を開始できる日付を指定
  - 形式は“year-month-day”
- 有効期間
  - 利用者が eduroam を使用できる期間を指定
  - 期間は使用開始日の 0:00 からの日数となる
  - 機関の指定は、日・週・月のいずれかを選択し、選択した行で数値を選択
- 発行アカウント数
  - 一括して発行するアカウント数を指定

3.3.3 出力

指定したアカウント数分下記情報が表示されます。

- Account
  - 発行されたアカウント名
- パスワード
  - 発行されたアカウント用のパスワード

3.4 アカウントロック／解除

アカウントごとの使用禁止、解除を行います。

3.4.1 手順

2. アカウント一覧の表示
   - 使用可能期間内のアカウントの一覧が表示されます
3. アカウント毎にロック（使用禁止）、ロックしないを選択
4. “send”をクリック
5. 操作後の状態が表示されます

3.4.2 アカウント一覧

- CenterLock
  - 代理認証システム管理者が使用を禁止にしたアカウントは“LOCKED”と表示
- Lock
  - 使用禁止されているアカウントは、チェックがついています
- アカウント名

- 使用期間内のアカウントのアカウント名

3.4.3 使用禁止・解除の指定

- 使用禁止
  - アカウント一覧の“Lock”をチェック
- 使用禁止の解除
  - アカウント一覧の“Lock”のチェックを外す

3.4.4 操作後アカウント一覧

- CenterLock
  - 代理認証システム管理者が使用を禁止にしたアカウントは“LOCKED”と表示
- Lock
  - 使用が禁止されているアカウントは、“”LOCKED”と表示
- アカウント名
  - 使用期間内のアカウントのアカウント名

3.5 利用者パスワード変更

利用者個人のパスワードの変更を行います。

新しいパスワードを入力するか、自動を選択した上で、変更対象の利用者を選び、画面下部の newpassword をクリックします。

第4章　機関管理

この章では機関管理の各操作を説明します。
対象となる機関管理者は自機関の機関管理者です。

4.1 管理者一覧

登録されている機関管理者の一覧が表示されます。

4.1.1 列の説明

- id
  - システムが採番した一意識別子
- UID
  - 登録された機関管理者の ID
- ロック
  - 機関管理者が使用禁止にした機関管理者は“LOCKED”と表示
- センターロック
  - 代理認証システム管理者が使用禁止にした機関管理者は“LOCKED”と表示
- 登録日
  - 機関管理者が追加された時点のタイムスタンプ

4.2 管理者追加

自機関の機関管理者を追加する際に使用します。

4.2.1 手順

1. 発行関連のパラメータを入力
2. “send”をクリック
3. 操作の結果が表示される

4.2.2 入力

機関管理者追加時には下記を指定してください。

- UID
  - 機関管理者がシステムに login する際に使用する ID。
  - システムを利用する全機関で一意な識別子になります。
  - a-z, A-Z, 0-9, ‘-’, ‘_’が使用可能、先頭の文字は a-z, A-Z に限定、最後の文字に ‘_’, ‘-’は使用できません。
- 管理者名

- 機関管理者の名前を入力
- a-z, A-Z, 0-9, '-', '_' , ' 'が使用可能、先頭の文字は a-z, A-Z,0-9 に限定、最後の文字に ' 'は使用できません。

- パスワード
  - 機関管理者がシステムに login する際に使用するパスワード
  - a-z, A-Z, 0-9, '-', '_'が使用可能
- パスワード自動生成
  - これをチェックすると使用するパスワードが自動生成されます (推奨)

4.2.3 出力

登録が成功した場合、下記情報が表示されます。

- Administrator UID
  - 登録した UID
- Administrator Name
  - 登録した管理者名
- Password
  - パスワード自動生成を指定した場合に発行されたパスワード

登録の失敗の原因例としては下記があります。

- 必須項目入力なし
  - 入力項目が不足している
- password error
  - パスワードを 2 度入力するが、一致していない
- その他
  - すでに UID が使用されている

4.3 管理者のロック／解除

機関管理者の使用禁止、使用禁止の解除を行います。

4.3.1 手順

1. 機関管理者一覧の表示
   - 機関管理者の一覧が表示されます
2. 機関管理者毎にロック(使用禁止)、ロックしないを選択
3. "send"をクリック
4. 操作後の状態が表示されます

4.3.2 機関管理者一覧

- CenterLock
  - 代理認証システム管理者が使用禁止にした機関管理者は"LOCKED"と表示

- Lock
  - 使用禁止されている機関管理者は、チェックがついています
- UID
  - 機関管理者の ID
- 名前
  - 機関管理者の登録されている名前

4.3.3 使用禁止・解除の指定

- 使用禁止
  - 機関管理者の“Lock”をチェック
- 使用禁止の解除
  - 機関管理者の“Lock”のチェックを外す

4.3.4 操作後の機関管理者一覧

- CenterLock
  - 代理認証システム管理者が使用を禁止にした機関管理者は“LOCKED”と表示
- Lock
  - 使用が禁止されている機関管理者は、“”LOCKED”と表示
- UID
  - 機関管理者の ID
- 名前
  - 機関管理者の登録されている名前

4.4 自パスワード変更

login している機関管理者のパスワードを変更します。

4.4.1 手順

1. 旧パスワードと新パスワードを入力
   - パスワードには a-z, A-Z, 0-9, ‘-’, ‘_’が使用可能
   - 他のシステムと同じ、または、類推しやすいパスワードを使わない
   - パスワードは英数字 8 文字以上が必要
2. “send”をクリック
3. 操作の結果が表示されます

4.5 パスワード設定

自機関の機関管理者のパスワードを変更します。

4.5.1 手順

1. 新パスワードを入力
   - パスワードには a-z, A-Z, 0-9, ‘-’, ‘_’が使用可能
   - 他のシステムと同じ、または、類推しやすいパスワードを使わない
   - パスワードは英数字 8 文字以上が必要
   - パスワード自動生成をチェックすると新パスワードを自動的に生成します (推奨)
2. パスワードを設定するユーザを選択
3. “send”をクリック
4. 操作結果が表示されます
   - パスワード自動生成をチェックした場合生成された新パスワードが表示されます

4.6 オンラインサインアップ機能設定

オンラインサインアップ機能を設定するサブメニューです。初期状態では、この機能は無効になっています。

オンラインサインアップ機能を有効にすると、個々の利用者が機関のメールアドレスを利用して、eduroam アカウントの申請を行えるようになります。

申請があった場合、事前に登録したメールアドレスに対して通知メールが送られます。管理者はその内容を見て承認・拒否操作を行います。

4.7 ログアウト

機関管理者メニューからログアウトします。クリック後に表示されるログインダイアログでキャンセル操作するか、代理認証システムのウィンドウ(タブ)をクローズしてください。

明示的にログアウト操作をしない場合、ブラウザを終了するまで、ログインされた状態が維持されます。

付録A　ロギング

代理認証システムでは、誤った操作によるトラブルの追跡や、不正利用時の保全に備えて、下記のログが記録されています。

- アカウント管理
  - アカウント発行
  - パスワードダウンロード
  - アカウントロック／ロック解除
  - RADIUS サーバのログ
    - RADIUS の認証成功・失敗
    - RADIUS のアカウンティング
- 機関管理
  - 機関管理者の登録
  - 機関管理者のパスワード変更操作
  - 機関管理者のロック／ロック解除