

府省認証局の詳細仕様

平成13年8月2日

基本問題専門部会了承

1	はじめに.....	1
2	システム機能仕様.....	1
	(1) 府省認証システムの機能.....	1
	ア 鍵管理サブシステム.....	1
	イ 証明書発行サブシステム.....	3
	ウ 証明書失効サブシステム.....	6
	エ ポリシ管理サブシステム.....	7
	オ 監査ログ管理サブシステム.....	8
	カ バックアップ・リカバリサブシステム.....	10
	キ アーカイブサブシステム.....	11
	ク アクセスコントロールサブシステム.....	13
	ケ スケジュール管理サブシステム.....	14
	コ システム環境設定サブシステム.....	15
	(2) 府省認証局リポジトリの機能.....	16
	ア サービス制御サブシステム.....	16
	イ 認証サブシステム.....	18
	ウ アクセス制御サブシステム.....	19
	エ ディレクトリ情報管理サブシステム.....	24
	オ 名前管理サブシステム.....	25
	カ 分散管理サブシステム.....	26
	キ バックアップ・リカバリサブシステム.....	27
	ク ログ出力サブシステム.....	28
	ケ 運用管理サブシステム.....	30
	(3) 稼動状況監視・ネットワーク監視機能.....	34
	ア 稼動状況監視.....	34
	イ ネットワーク監視.....	34
3	システム技術仕様.....	35
4	諸規程.....	36
	(1) 認証業務の運営方針.....	36

(2) 整備する規程、マニュアル等.....	36
ア 証明書管理に関する事項.....	36
イ システム運用管理に関する事項.....	36
ウ 各種業務管理に関する事項.....	36
エ 危機管理に関する事項.....	36
オ セキュリティ管理に関する事項.....	36

「政府認証基盤の基本的な仕様」(平成12年7月27日行政情報システム各省庁連絡会議幹事会了承)に基づく詳細な仕様は、以下のとおりとする。

1 はじめに

本仕様は、先導的に整備した府省認証局及びブリッジ認証局の構築・実証実験を踏まえ、府省認証局の詳細な仕様を取りまとめたものである。

2 システム機能仕様

府省認証局は、府省認証システム及び府省認証局リポジトリにより構成し、各システムを運用するために必要な機能は以下のとおりとする。

(1) 府省認証システムの機能

ア 鍵管理サブシステム

府省認証システムの秘密鍵を管理するとともに、秘密鍵を使った署名を行う。

(ア) 鍵生成

府省認証システムの鍵ペアを生成する。鍵生成及び保管には、FIPS140-1レベル3相当以上のハードウェア鍵管理装置(HSM: Hardware Security Module)を用いる。

府省認証システムの鍵ペアは、複数の権限者の操作により生成する。

(イ) 署名

HSMに保管している府省認証システムの秘密鍵を用いて署名を行う。

(ウ) 鍵バックアップ

HSMに保管されている府省認証システムの秘密鍵を複数の権限者の操作によりバックアップする。

なお、秘密鍵のバックアップでは、データの分割、暗号化等を行う。

(エ) 鍵リカバリ

複数の権限者の操作により、HSM の秘密鍵を復元する。

(オ) 鍵廃棄

HSM に保管されている府省認証システムの秘密鍵を、複数の権限者の操作により廃棄する。

バックアップしている秘密鍵も痕跡が残らないように廃棄する。

(カ) 鍵更新

府省認証システムの新しい鍵ペアを生成後、証明書発行サブシステムに以下の指示を行う。

- 新しい自己署名証明書 (NewWithNew) の生成指示
- 古い世代の鍵と新しい世代の鍵を紐付けるリンク証明書 (OldWithNew、NewWithOld) の生成指示

(キ) エンドエンティティ鍵生成

エンドエンティティの鍵ペアを生成する。生成した鍵ペアは、記憶媒体に保管する。

(ク) エンドエンティティ鍵保護

生成されたエンドエンティティの秘密鍵の漏えい及び改ざんを防止する。

イ 証明書発行サブシステム

証明書発行要求（CSR：Certificate Signing Request）の受付、証明書等の生成指示、生成、出力等を行う。

（ア）証明書発行要求（CSR）受付

証明書発行要求（CSR）を受け付け、含まれる署名に基づき、改ざんの有無を検証するとともに、内容の検証を行う。

（イ）証明書生成指示

以下の証明書生成指示を行う。

- 自己署名証明書生成指示

鍵管理サブシステムより公開鍵を受け取り、自己署名証明書生成指示を行う。

- リンク証明書生成指示

鍵管理サブシステムより新旧の公開鍵を受け取り、以下の2種類のリンク証明書生成指示を行う。

- ・古い世代の公開鍵を新しい世代の秘密鍵で署名した証明書
(OldWithNew)
- ・新しい世代の公開鍵を古い世代の秘密鍵で署名した証明書
(NewWithOld)

- 官職証明書生成指示

鍵管理サブシステムより公開鍵を受け取り、官職証明書生成指示を行う。

- 相互認証証明書及び証明書発行要求（CSR）生成指示

相互認証する相手認証局からの証明書発行要求（CSR）に基づき相

相互認証証明書生成指示を行う。また、相互認証する相手認証局への証明書発行要求（CSR）の生成指示を行う。

なお、証明書発行要求（CSR）は、PKCS#10 で規定されたフォーマットで ASN.1 エンコードされたバイナリフォーマットとし、認証局の公開鍵、その他の情報を含む発行要求として外部記憶媒体により授受を行う。

- 相互認証証明書ペア生成指示

相互認証する相手認証局との間で相互に発行した相互認証証明書に基づき相互認証証明書ペア生成指示を行う。

- カスタム証明書生成指示

鍵管理サブシステムより公開鍵を受け取り、自己署名証明書、リンク証明書、官職証明書、相互認証証明書及び相互認証証明書ペア以外に府省認証システムが発行する証明書（SSL 認証に用いる証明書等）について証明書生成指示を行う。

（ウ）証明書及び証明書発行要求（CSR）生成

証明書生成指示、各種プロファイル等に基づき各種証明書及び証明書発行要求（CSR）を生成する。

（エ）相互認証証明書ペア生成

相互認証証明書ペア生成指示に基づき相互認証証明書ペアを生成する。

（オ）証明書及び証明書発行要求（CSR）出力

証明書及び証明書発行要求生成機能、相互認証証明書ペア生成機能から受け取った証明書、証明書発行要求（CSR）、相互認証証明書ペアを府省認証システム外（府省認証局リポジトリ、外部記憶媒体等）へ出力する。外部記憶媒体への出力形式は以下のとおりとする。

- 証明書
 - DER 形式
 - base64 形式
 - PKCS#7 形式
- 証明書発行要求 (CSR)
 - PKCS#10 形式
- 相互認証証明書ペア
 - DER 形式

(カ) 秘密鍵の暗号モジュールへの格納

必要に応じ、官職証明書等に対応する秘密鍵を IC カード等、FIPS140-1 レベル 2 相当の暗号モジュールに出力する。

ウ 証明書失効サブシステム

証明書発行サブシステムで発行した証明書の失効並びに認証局失効リスト及び証明書失効リストの発行を行う。

(ア) 証明書失効要求受付

証明書失効要求を受け付ける。

(イ) 証明書ステータス変更

府省認証システムが発行した証明書のステータスを「失効」状態へ変更する。ただし、失効した証明書を有効な状態に戻すことは不可能とする。

(ウ) 認証局失効リスト (ARL : Authority Revocation List) ・ 証明書失効リスト (CRL : Certificate Revocation List) 生成

証明書失効要求と ARL プロファイル、CRL プロファイル等に基づき、認証局失効リスト、証明書失効リストを生成する。

認証局失効リスト及び証明書失効リストは、証明書ステータスの変更による即時生成及びスケジュール管理サブシステムによる定期的な生成を可能とする。

(エ) 認証局失効リスト (ARL) ・ 証明書失効リスト (CRL) 出力

認証局失効リスト及び証明書失効リストを府省認証システム外 (府省認証局リポジトリ、外部記憶媒体等) へ出力する。

エ ポリシ管理サブシステム

証明書及び失効リストのプロファイル設定、変更等を行う。

(ア) 自己署名証明書プロファイル設定・参照

自己署名証明書発行時に、自己署名証明書プロファイルの設定を行う。自己署名証明書発行後は、自己署名証明書プロファイルの参照を行う。

(イ) 相互認証証明書プロファイル設定・変更

相互認証証明書プロファイルの設定及び変更を行う。

(ウ) 官職証明書プロファイル設定・変更

官職証明書プロファイルの設定及び変更を行う。

(エ) 認証局失効リスト (ARL) プロファイル設定・変更

ARL プロファイルの設定及び変更を行う。

(オ) 証明書失効リスト (CRL) プロファイル設定・変更

CRL プロファイルの設定及び変更を行う。

(カ) カスタム証明書プロファイル設定・変更

(ア) ~ (ウ) 以外に府省認証システムが発行する証明書 (SSL 認証に用いる証明書等) について、証明書プロファイルの設定及び変更を行う。

オ 監査ログ管理サブシステム

府省認証システムがセキュアに運用されていることを監査するために必要な情報の採取及び管理を行う。

(ア) 監査ログ生成

監査の対象となる以下の事象が発生した場合に、当該事象を監査ログとして生成し、記録する。

- 府省認証システム導入設定
- 操作員登録、権限設定
- ポリシ設定/変更
- 府省認証システム起動/停止
- バックアップ/リカバリ実行
- 証明書要求の発行
- 証明書の発行
- 証明書の失効
- 認証局失効リスト（ARL）の発行
- 証明書失効リスト（CRL）の発行
- 鍵の操作
- 府省認証システムにおけるエラーの発生

また、監査ログには少なくとも以下の情報を記録する。

- 事象の種類
- 事象が発生した日付及び時刻
- 各種処理の結果
- 事象の発生元の識別情報（操作員、システム名等）

(イ) 監査ログ出力

監査ログを記憶媒体に出力する。

監査ログの消失を防ぐため、書き込みエラーが発生した場合には警告を

出し、警告に対する対処がなされるまで、監査の対象となる事象に係る処理を受け付けない。

(ウ) 監査ログ保護

監査ログの削除、改ざん等を検知するため、署名を行う。

(エ) 監査ログ参照

監査ログから内容を読み込み、表示する。

(オ) 監査ログ検証

監査ログの削除、改ざん等が行われていないことを検証する。

(カ) 監査ログ検索

監査ログを参照する際に、以下の項目により条件を指定して検索する。

- 事象の種類
- 事象が発生した日付及び時刻
- 各種処理の結果
- 事象の発生元の識別情報（操作員、システム名等）
- 監査ログの状態(削除、改ざん等)

(キ) 監査ログ保管

監査ログを保管するため、一部又は全ての監査ログを外部記憶媒体に複写又は移動する。また、外部出力データの削除、改ざん等を検知するため、署名を行う。

カ バックアップ・リカバリサブシステム

府省認証システムの障害に備えて、システムの復旧に必要なデータのバックアップを行う。障害が発生した場合には、バックアップをリストアすることにより府省認証システムを復旧する。

(ア) バックアップ

バックアップデータとして、操作員情報、権限情報、証明書、CRL / ARLのプロファイル、運用パラメータ等、府省認証システムの復旧に必要な情報を外部記憶媒体に出力する。

(イ) リカバリ

バックアップデータをリストアし、府省認証システムをバックアップが作成されたときの状態に復旧する。

(ウ) バックアップデータ保護

バックアップデータの削除、改ざん等を検知するため署名を行うとともに、セキュリティ上重要なバックアップデータは暗号化する。また、署名、暗号化の鍵はセキュアに管理する。

(エ) バックアップデータ検証

バックアップデータの削除、改ざん等が行われていないことを検証する。

キ アーカイブサブシステム

府省認証システムが発行した証明書及び CRL / ARL の履歴を管理する。

(ア) アーカイブデータ生成

以下のデータをアーカイブデータとして生成し、記録する。

- 証明書の発行履歴
- CRL / ARL の発行履歴
- 起動停止ログ
- 操作ログ

また、アーカイブデータには少なくとも以下の情報を記録する。

- 事象の種類
- 事象が発生した日付及び時刻
- 各種処理の結果
- 事象の発生元の識別情報（操作員、システム名等）

(イ) アーカイブデータ出力

アーカイブデータを記憶媒体に出力する。

(ウ) アーカイブデータ保護

アーカイブデータの削除、改ざん等を検知するため、署名を行う。

(エ) アーカイブデータ参照

アーカイブファイルから内容を読み込んで表示する。

(オ) アーカイブデータ検証

アーカイブデータの削除、改ざん等が行われていないことを検証する。

(カ) アーカイブデータ検索

アーカイブデータを参照する際に、以下の項目により条件を指定して検索する。

- 事象の種類
- 事象が発生した日付及び時刻
- 各種処理の結果
- 事象の発生元の識別情報（操作員、システム名等）
- アーカイブデータの状態(削除、改ざん等)

(キ) アーカイブデータ保管

アーカイブデータを保管するため、一部又は全てのアーカイブデータを外部記憶媒体に複写又は移動する。また、外部出力データの削除、改ざん等を検知するため、署名を行う。

ク アクセスコントロールサブシステム

あらかじめ定められた府省認証システムの運用に関する操作員の役割とセキュリティ要件に基づき、府省認証システムへのアクセスを操作員識別情報等によって制御する。

(ア) 操作員登録・削除

府省認証システムの操作員の登録及び削除を行う。

(イ) 権限設定

府省認証システムに対する役割を設定し、役割に応じた権限の付与及び削除を行う。

(ウ) 権限情報保護

登録された操作員情報及び操作員に割り当てた権限情報の漏えい及び改ざんを防止する。

(エ) 操作員認証

操作員の認証及び識別を行う。

(オ) アクセス制御

要求された操作について、要求元の操作員に権限が与えられているかどうか確認し、結果を返す。

ケ スケジュール管理サブシステム

府省認証システムをあらかじめ定めたスケジュールで運用する。

(ア) スケジュール設定

以下のスケジュールの設定、変更及び削除を行う。

- 認証局失効リスト (ARL) 生成
- 証明書失効リスト (CRL) 生成

(イ) スケジュール実行

あらかじめ設定されたスケジュールを実行する。

コ システム環境設定サブシステム

府省認証システムの運用に必要なパラメータの設定・参照を行う。

(ア) 運用パラメータ設定

システム運用に関するパラメータの設定及び変更を行うとともに、パラメータの漏えい及び改ざんを防止する。

(イ) 運用パラメータ参照

運用パラメータ設定機能で設定したパラメータを参照する。

(2) 府省認証局リポジトリの機能

ア サービス制御サブシステム

府省認証局リポジトリにアクセスするクライアントからの要求を受け取り、その要求の処理結果を要求元であるクライアントに返す。

(ア) バインドとアンバインド

証明書の検索や失効情報の登録など、クライアントが府省認証局リポジトリに対して何らかの操作を行う場合、府省認証局リポジトリはクライアントに対し、バインド操作を要求する。

クライアントから“バインド要求”を受け取った府省認証局リポジトリ（ディレクトリサーバ）は、プロトコルセッションを確立する。さらに、要求を出したクライアントの認証を行い、認証の結果を示す“バインド応答”をクライアントに返す。

一方、府省認証局リポジトリに対する操作を終了する場合、クライアントは“アンバインド要求”を発行し、その時点でプロトコルセッションが終了したものであるとして府省認証局リポジトリとのコネクションを閉じる。

(イ) 検索

クライアントから与えられた条件に該当する各種証明書、失効情報などをクライアントに返す。

クライアントは、証明書に記述される発行者（issuer）や所有者（subject）を条件として、証明書を発行したCAエントリ又は所有者によって示されるエンドエンティティエントリを検索する。

(ウ) エントリ追加

CAエントリ、エンドエンティティエントリを追加する。たとえば、ある府省において新たにCAを立てる場合、そのCAを表すエントリを府省認証局

リポジトリに追加する。また、官職が新たに設けられた場合、その官職を表すエントリを府省認証局リポジトリに追加する。

(エ) エントリ削除

CA エントリ、エンドエンティティエントリを削除する。たとえば、ある府省においてそれまで運営されていた CA を廃止する場合、その CA を表すエントリを府省認証局リポジトリから削除する。また、官職が廃止された場合、その官職を表すエントリを府省認証局リポジトリから削除する。

(オ) エントリ変更

各種証明書、失効情報をエントリの属性値として登録する。また、失効情報の更新等により認証情報を更新した場合、その認証局を示すエントリの属性値を更新する。

(カ) 識別名変更

CA エントリ、エンドエンティティエントリの識別名を変更する。たとえば、府省の名称変更又は各府省に属する部局の名称変更があった場合、その府省又は部局を表すエントリの識別名を変更する。

(キ) レプリケーション

府省認証局リポジトリに対して成功した全ての追加、削除、更新操作内容のうち、「政府認証基盤相互運用性仕様書」(平成13年4月25日基本問題専門部会了承)(以下「相互運用性仕様書」という。)における「5.5.2 府省 CA リポジトリの統合リポジトリへの複製」で定められている複製情報のみを、TLS プロトコルを用いてブリッジ認証局の統合リポジトリに自動複製する。

イ 認証サブシステム

府省認証局リポジトリを利用するクライアントが真正なクライアントであるかどうかを確認するための認証を行う。

(ア) 認証

クライアントが提示した認証情報を府省認証局リポジトリに格納される認証情報と比較し、提示された情報があらかじめ格納されている認証情報と一致すれば府省認証局リポジトリの利用を許可し、一致しなければ府省認証局リポジトリの利用を拒否する。

府省認証局リポジトリが有する認証レベルとしては、認証なし、名前だけの認証、パスワード認証、証明書による TLS 厳密認証の 4 段階がある。TLS 厳密認証の場合、RFC2829 及び RFC2830 に定める規定を満足するものとする。

府省認証局リポジトリが格納する情報に対するクライアントの操作の種類毎に、必要とする認証レベルを以下のとおりとする。

- 検索操作：認証なしとする。
- 更新操作：不特定多数のクライアントのアクセスが想定される場合には、原則として TLS 厳密認証とする。その他の場合はパスワード認証とする。

なお、TLS 厳密認証を行う場合に必要な鍵の管理を行い、その証明書は府省認証システムが発行する。

ウ アクセス制御サブシステム

府省認証局リポジトリが格納する情報に対し、あらかじめ登録されたアクセス制御情報に基づきアクセス制御を行う。アクセス制御情報自体もディレクトリ上の属性として登録する。

なお、府省認証局リポジトリでは、アクセス制御機構として、ディレクトリ標準(ITU-T Rec. X.501 | ISO/IEC 9594-2)の基本アクセス制御(Basic Access Control)を利用する。

(ア) アクセス制御の設定手段

以下の3種類の手段を用いてアクセス行う。

- prescriptiveACI

ディレクトリ情報ツリーのサブツリーを対象とし、共通のアクセス制御情報を設定する手段である。サブツリーの頂点に該当するエントリに prescriptiveACI を設定することによって、サブツリーに含まれる全てのエントリに対するアクセス制御情報を設定する。

- entryACI

各々のエントリ個別のアクセス制御情報を設定する手段である。各エントリに entryACI を設定することによって、エントリ単位でのアクセス制御情報を設定する。

- subentryACI

管理領域全般に渡る運用情報を管理するサブエントリに対するアクセス制御情報を設定する手段である。管理領域の頂点に該当するエントリに subentryACI を設定することによって、サブエントリに対するアクセス制御情報を設定する。

(イ) 基本アクセス制御

基本アクセス制御では、以下の項目を利用することにより、クライアントから府省認証局リポジトリに対する操作の許可又は拒否の判断を行う。

- ディレクトリ情報中で、アクセス保護の対象となる部分（エントリ、属性、属性値）を表す保護項目
- クライアントの識別名及び認証レベル
- 要求された操作の処理に必要なアクセス許可種別
- アクセス制御情報項目

A アクセス許可種別

クライアントからの操作要求に対してアクセス権を判定する過程には以下の二つのフェーズがある。

(a) エントリへのアクセス処理

(b) エントリがもつ個々の属性へのアクセス処理

エントリアクセスに対するアクセス許可種別を表1に示す。

表1 エントリアクセスに対するアクセス許可種別

許可種別	意味
Read	エントリ名を明らかに指定した参照
Browse	エントリ名を指定しない参照
Add	エントリの追加
Remove	エントリの削除
Modify	エントリの更新
Rename	エントリの識別名の更新
DiscloseOnError	エラー結果でのエントリ名の開示
Export	エントリ移動時の移動元での削除
Import	エントリ移動時の移動先での追加
ReturnDN	正常結果でのエントリ名の開示

属性アクセスに対するアクセス許可種別を表 2 に示す。

表 2 属性アクセスに対するアクセス許可種別

許可種別	意味
Compare	比較操作での属性や属性値の比較
Read	検索操作などでの属性や属性値の参照
FilterMatch	検索操作でのフィルタとしての比較
Add	属性や属性値の追加
Remove	属性や属性値の削除
DiscloseOnError	エラー結果での属性や属性値の開示

各保護項目に対して、これらの各種別の許可又は拒否をアクセス制御情報項目の形式で記述し、ディレクトリ内に格納しておくことにより、アクセス制御処理を行う。

B アクセス制御情報項目

アクセス制御情報は、ACI 運用属性の属性値であるアクセス制御情報項目の集合として表現される。各々のアクセス制御情報項目では、特定のクライアントから特定の保護項目へのアクセスの許可又は拒否を定める情報を保持する。

アクセスの可否判断は、クライアントからの要求を満たすために対象となるクライアント種別、保護項目、許可種別のいずれかが関連する全てのアクセス制御情報項目を利用して判定する。

アクセス制御情報項目を構成する要素を以下に示す。

(a) 識別タグ

アクセス制御情報項目の管理に用いるための識別子。

(b) 優先順位

アクセス制御情報項目の優先度を表す値。複数のアクセス制御情報項目の中で相反する定義があった場合、この優先順位の値が高いものを最優先する。

(c) 認証レベル

クライアントに要求される認証レベルを規定する。この設定値よりもレベルの低い認証を経たクライアントからアクセスされた場合、そのアクセスは拒否される。

(d) クライアント種別

制御の対象となるクライアントを規定する。クライアントの指定方法としては、名前による単一のクライアントを指定するだけでなく、グループ、サブツリーによる複数のクライアントを一括して指定することも可能とする。

(e) 保護項目

制御の対象となる情報を規定する。エントリ、属性、属性値単位での指定を可能とする。

(f) 許可又は拒否

クライアント種別に指定されたクライアントが保護項目に指定された項目にアクセスする場合の、各種アクセス許可種別による許可又は拒否を設定する。

複数のアクセス制御情報において、同じ優先順位で矛盾する設定がされたとき、拒否の設定を優先する。

(ウ) 府省認証局の操作員及び府省認証システムに対するアクセス制御

府省認証局リポジトリにアクセスするクライアントが府省認証局の操作員又は府省認証システムである場合、府省認証局リポジトリが管理する情報へのアクセスを以下のように制限する。

(a) その府省認証局自身を表すエントリ配下の全ての情報に対して、更

新操作を可能とする。

(b) 他の操作員の情報を除いた府省認証局リポジトリが管理する全ての情報に対して、検索操作を可能とする。

(c) 上記以外の操作は禁止する。

(エ) その他クライアントに対するアクセス制御

府省認証局リポジトリにアクセスするクライアントが府省認証局の操作員、府省認証システムのいずれでもない場合、府省認証局リポジトリが管理する情報に対する検索操作のみを許可する。

エ ディレクトリ情報管理サブシステム

各府省内の CA、組織、エンドエンティティの情報を、ディレクトリシステムにおけるエントリとして格納する。

さらに、府省認証局リポジトリにアクセスするクライアントからの要求をディレクトリ上に適切に反映し、反映した結果をクライアントに返す。

ディレクトリに格納される情報については、相互運用性仕様書における「7.12.3 統合リポジトリに格納される情報」に示すとおりとする。

オ 名前管理サブシステム

各府省内の CA、組織、エンドエンティティの情報を、全体として矛盾のない単一のディレクトリ情報ツリーとして管理する。また、各エントリを一意に特定するための識別名を管理し、識別名から対応するエントリ情報を取得する。これらにより、クライアントからの要求に応じて以下の判定を行う。

なお、リポジトリ内に対象となるエントリが存在しない場合及び識別名が重複する場合にはエラーを返す。

- 検索要求を受け取った場合、検索の基底となるエントリがリポジトリ内に存在するか否かを判定する。
- 更新要求を受け取った場合、更新対象となるエントリがリポジトリ内に存在するか否かを判定する。
- 追加要求を受け取った場合、新規追加されるエントリの直接上位となるエントリが存在するか否かを判定する。さらに、新規追加されるエントリが、他のエントリと重複する識別名をもつかどうかを判定する。
- 識別名変更要求を受け取った場合、変更対象となるエントリがリポジトリ内に存在するか否かを判定する。さらに、新しい識別名のエントリの直接上位となるエントリが存在するか否かを判定し、新しい識別名が他のエントリと重複しないことを判定する。
- 削除要求を受け取った場合、削除対象となるエントリがリポジトリ内に存在するか否かを判定する。

カ 分散管理サブシステム

複数のリポジトリと協調して、クライアントからの要求に応える。

府省認証局リポジトリにおいて、複数のリポジトリが個々に管理するディレクトリ情報ツリーを見かけ上単一のディレクトリ情報ツリーとして見せるために、府省認証局リポジトリから見た他のリポジトリとの関係を“知識参照”として管理する。知識参照の具体的な内容は、相互運用性仕様書における「7.12.3.8 リフェラルエントリ」において定義する ref 属性として管理される GPKI 外のリポジトリへのアクセスポイント情報と、referral エントリの識別名として管理されるコンテキストプレフィクスからなる。

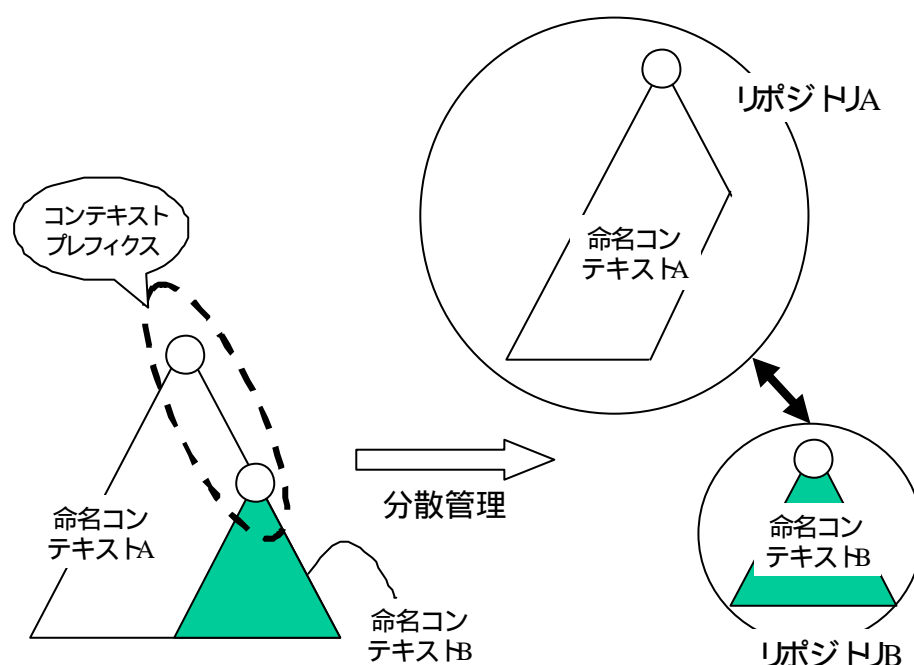


図1 命名コンテキストとコンテキストプレフィクス

クライアントから与えられた識別名を解析する過程で知識参照を得た場合、リフェラルを返す。一方、知識参照を得られなかった場合、ローカルに処理可能であると判定する。

キ バックアップ・リカバリサブシステム

府省認証局リポジトリの障害に備えて、復旧に必要なデータのバックアップを行う。障害が発生した場合には、バックアップをリストアすることにより府省認証局リポジトリを復旧する。

(ア) バックアップ出力

あらかじめ定められたスケジュールに沿って、府省認証局リポジトリが管理・格納する全ての情報を退避する。

(イ) ジャーナル出力

府省認証局リポジトリが管理・格納する情報に対して、最後にバックアップされた時点以降の更新差分情報を、ジャーナルとして出力する。

(ウ) 復旧

上記の機能を用いたバックアップファイル及びジャーナルファイルから障害発生時前の状態に復元する。

ク ログ出力サブシステム

アクセスログ、操作ログ、更新ログ及びエラーログを出力する。

(ア) アクセスログ

府省認証局リポジトリに対する全てのアクセスについてログを採取する。

以下に例を示す。

- アクセス時刻
- プロセス ID
- クライアントのアドレス (ドメイン名又は IP アドレス)
- 接続状態
- 同時接続数

(イ) 操作ログ

府省認証局リポジトリに対する全ての操作についてログを採取する。以下に例を示す。

- 操作時刻
- プロセス ID
- 操作員情報
- 操作種別
- 操作結果
- TAT

(ウ) 更新ログ

府省認証局リポジトリに対して成功した全ての更新操作についてログを採取する。以下に例を示す。

- 更新時刻
- 対象エントリ
- 更新内容

(エ) エラーログ

府省認証局リポジトリに何らかの障害が発生した場合、その障害の内容を示すログを採取する。以下に例を示す。

- 障害発生時刻
- プロセス ID
- 障害内容

ケ 運用管理サブシステム

リポジトリの運用に関わる機能を提供する。

(ア) ディレクトリサーバの起動・停止

ディレクトリサーバの起動、停止を行う。

(イ) ディレクトリサーバの動作状態出力

ディレクトリサーバが正常に動作しているか否かを外部からモニタリングする。

(ウ) バックアップ・スケジュール設定

府省認証局リポジトリが管理する情報の自動バックアップの設定を行う。
また、バックアップファイルの出力先を指定する。

(エ) ジャーナル出力設定

ジャーナルファイルの出力先を指定する。

(オ) ログ出力

各ログファイルの出力先を指定する。

(カ) MIB 出力

必要に応じ、府省認証局リポジトリの利用統計情報を MIB として外部に出力する。

府省認証局リポジトリが出力する MIB は以下の三つのテーブルを含む。

- dsTable

ディレクトリサーバのリスト。各サーバの説明やエントリに関する統計情報の要約、キャッシュのパフォーマンス等が含まれる。

- dsAppIIfOpsTable

アクセス、操作、エラーの統計情報の要約を示す。

- dsIntTable

同じ管理領域にあるディレクトリサーバ間のインタラクションに関する情報を表す。

A dsTable

dsTable として出力する内容を表 3 に示す。

表 3 dsTable の内容

dsServerType	ビット列	そのサーバがフロントエンドゲートウェイか、バックエンドサーバか又はその両方かを示す
dsServerDescription	文字列	ディレクトリサーバのコメント
dsMasterEntries	整数	サーバのもつマスタエントリの数
dsCopyEntries	整数	サーバのもつコピーエントリの数
dsCacheEntries	整数	サーバのもつキャッシュエントリの数
dsCacheHits	整数	キャッシュエントリのヒット操作数
dsSlaveHits	整数	コピーエントリのヒット操作数

B dsAppIfOpsTable

dsAppIfOpsTable として出力する内容を表4に示す。このテーブルはプロトコル毎にもつ。

表4 dsAppIfOpsTable の内容

dsAppIfProtocolIndex	整数	テーブルのインデックス
dsAppIfProtocol	OID	http://www.isi.edu/in-notes/iana/assignments/protocol-numbers
dsUnauthBinds	整数	認証無し/匿名バインド要求の数
dsSimpleAuthBinds	整数	簡易認証バインド要求の数 (SASL-CRAM-MD5 含む)
dsStrongAuthBinds	整数	厳密認証バインド要求の数 (TLS や external 含む)
dsBindSecurityErrors	整数	認証エラーにより拒否されたバインド応答の数
dsInOps	整数	受信した操作数
dsReadOps	整数	受信した読み出し操作の数
dsCompareOps	整数	受信した比較操作の数
dsAddEntryOps	整数	受信したエントリ追加操作の数
dsRemoveEntryOps	整数	受信したエントリ削除操作の数
dsModifyEntryOps	整数	受信したエントリ更新操作の数
dsModifyDNOps	整数	受信した識別名変更操作の数
dsListOps	整数	受信した一覧操作の数
dsSearchOps	整数	受信した全ての検索操作の数
dsOneLevelSearchOps	整数	受信した onelevel 検索操作の数
dsWholeSubtreeSearchOps	整数	受信したサブツリー検索操作の数
dsReferrals	整数	応答した照会の数
dsChainigs	整数	応答した連鎖の数
dsSecurityErrors	整数	セキュリティエラーの数
dsErrors	整数	応答したエラーの数。セキュリティエラー、照会、部分的に処理した操作の数は含まない。
dsReplicationUpdatesIn	整数	供給側サーバから受けた/取得したレプリケーション更新の数
dsReplicationUpdatesOut	整数	消費側サーバに送った/取得されたレプリケーション更新の数

dsInBytes	整数	全ての受信バイト数
dsOutBytes	整数	全ての送信バイト数

C dsIntTable

dsIntTable として出力する内容を表 5 に示す。

他のディレクトリサーバとのインタラクションに関する統計情報をモニタする。このテーブルは常に直近の N 個のディレクトリサーバに関する情報を保持する。N はローカル定義の変数である。

表 5 dsIntTable の内容

dsIntIndex	整数	テーブルインデックス
dsDirectoryName	文字列	相手のディレクトリサーバの識別名
dsTimeOfCreation	時刻	このサーバに関するテーブルの作成時刻
dsTimeOfLastAttempt	時刻	このサーバに最後に通信した時刻
dsTimeOfLastSuccess	時刻	このサーバとの通信が最後に成功した時刻
dsFailuresSinceLastSuccess	整数	このサーバとの通信が最後に成功した後の、通信の失敗回数
dsFailures	整数	通算の失敗回数
dsSuccesses	整数	通算の成功回数
dsURL	URL	相手のサーバの URL

(3) 稼働状況監視・ネットワーク監視機能

ア 稼働状況監視

各サーバの稼働状況を常時監視し、以下の異常発生時に監視端末に通知する。

- サーバの稼働が停止した場合
- サーバに関する資源（CPU、メモリ、ディスク）の使用状況があらかじめ設定した閾値を超えた場合
- サーバ上で動作しているあらかじめ監視対象に定めたプロセスが異常終了した場合

イ ネットワーク監視

外部からのアクセスを監視し、不正アクセス検知時に監視端末に通知する。

3 システム技術仕様

府省認証システム及び府省認証局リポジトリの保有機能を実現し、政府認証基盤としての相互運用性を確保するための技術仕様については、相互運用性仕様書における「4 異なるPKIドメイン間の相互運用性」、「5 PKIドメイン内仕様」、「7 プロファイル」及び「8 付録」のとおりとする。

4 諸規程

(1) 認証業務の運営方針

府省認証局の認証業務の運営方針を「府省認証局CP/CPSガイドライン」(平成13年4月25日基本問題専門部会了承)に準拠して定める。

(2) 整備する規程、マニュアル等

府省認証局が認証業務を実施するに当たっては、認証業務の運営方針を踏まえ以下の事項についての規程、マニュアル等を整備する。

ア 証明書管理に関する事項

自己署名証明書、リンク証明書、相互認証証明書、官職証明書等の新規発行・失効・更新等に関する事項

イ システム運用管理に関する事項

リポジトリ更新、バックアップ、アーカイブ、稼動状況監視、保守点検、障害対策、機能強化、設定変更、ログ検査等に関する事項

ウ 各種業務管理に関する事項

組織体制、運用権限管理、教育管理、入退室管理、物理鍵管理、書類・データ管理、保管庫管理、ハードウェア・ソフトウェア保守運用管理、資産管理、テスト環境管理等に関する事項

エ 危機管理に関する事項

秘密鍵紛失・漏えい等による秘密鍵の直接的な危殆化、不正アクセス・不正操作等による秘密鍵の間接的な危殆化、災害等発生時の対応等に関する事項

オ セキュリティ管理に関する事項

情報セキュリティポリシーに基づく府省認証局における情報セキュリティポリシー実施手順