

# 政府認証基盤(GPKI)フォーラム 資料

2000年7月12日

(社)行政情報システム研究所

## 【目次】

### <1. 政府認証基盤構築の基本方針と検討範囲>

- 政府認証基盤の概要－全体像イメージ
- 政府認証基盤の整備・運営に当たっての基本方針
- 政府認証基盤の検討範囲

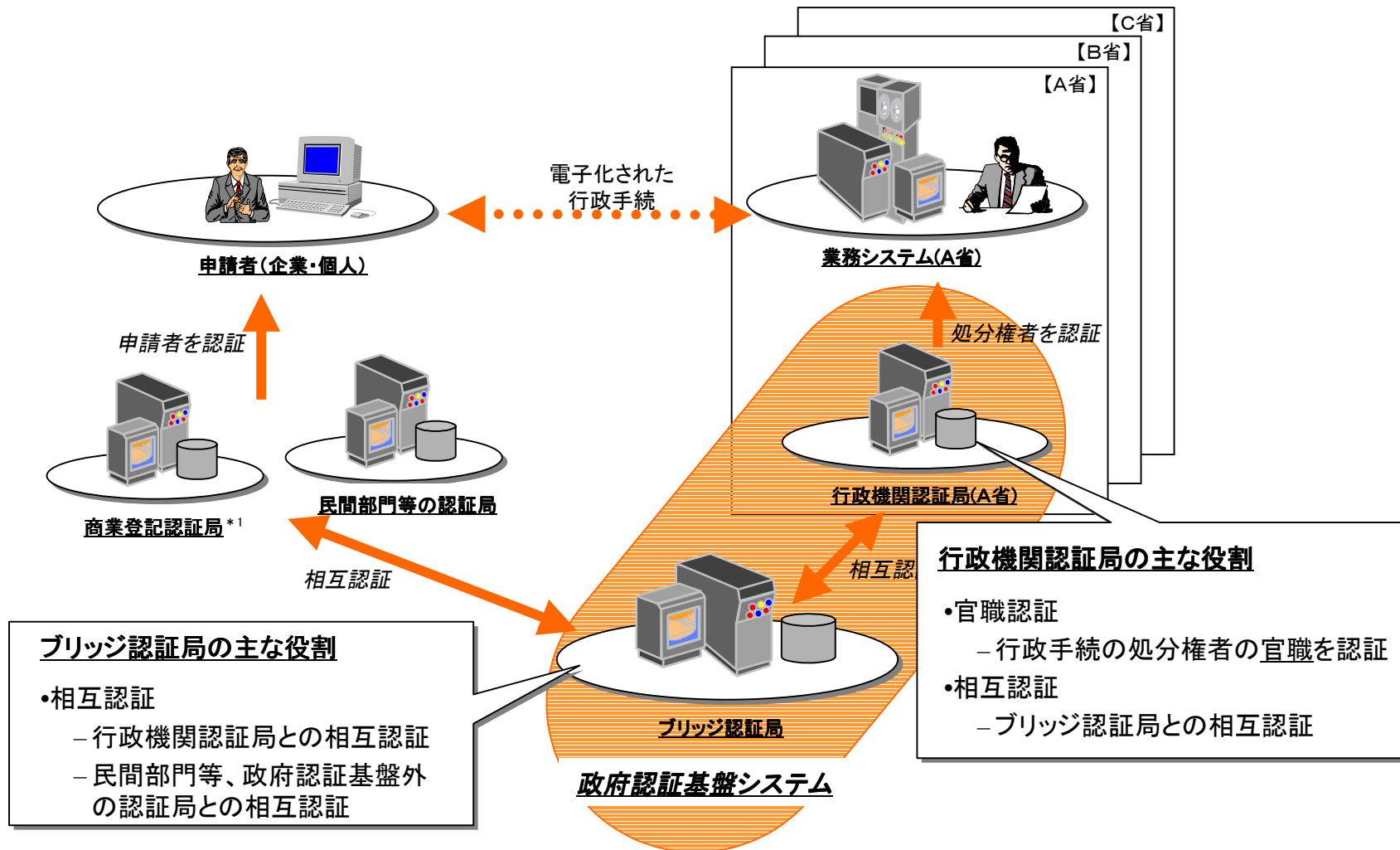
### <2. 政府認証基盤の詳細仕様の概要>

- 政府認証基盤の詳細構成
- 行政機関認証局のシステム機能構成
- 行政機関認証局のシステム機能－行政機関CAシステム
- 行政機関認証局のシステム機能－行政機関リポジトリ
- ブリッジ認証局のシステム機能構成
- ブリッジ認証局のシステム機能－BCAシステム
- ブリッジ認証局のシステム機能－BCAリポジトリ
- ブリッジ認証局のシステム機能－統合リポジトリ
- ブリッジ認証局のシステム機能－証明書検証システム
- 各システム構成要素の連携－各リポジトリへの認証情報の登録
- 各システム構成要素の連携－統合リポジトリへの認証情報の登録
- 各システム構成要素の連携－申請者証明書の有効性検証
- 各システム構成要素の連携－官職証明書の有効性検証
- 政府認証基盤運用方針・運用手続
- 政府認証基盤相互認証接続条件－全体概要
- 政府認証基盤相互認証接続条件－ブリッジ認証局と行政機関認証局との接続条件
- 政府認証基盤相互認証接続条件－民間認証局の政府認証基盤接続条件
- 政府認証基盤 施設設備/HW・SWの必要要件

## 1. 政府認証基盤構築の基本方針と検討範囲

## 政府認証基盤の概要 - 全体像イメージ

政府認証基盤は、各行政機関の認証局(以下「行政機関認証局」と)と、単一のブリッジ認証局から構成される。その全体像イメージ、及び行政機関認証局・ブリッジ認証局の主な役割は次のとおりである。



\*1 法務省「商業法人登記に基礎を置く電子認証」のために設置される認証局を指す。

## 政府認証基盤の整備・運営に当たっての基本方針

政府認証基盤の整備・運営に当たっての基本方針は次のとおりである。

### 【1】申請者の負担の軽減及び利便性の向上

- 広く利用されている国際的な標準に基づく仕様・技術を原則として採用し、現在の情報通信技術の環境に適合させる。
- 申請者が行政機関認証局から提供を受ける情報をブリッジ認証局から一元的に提供する。

### 【2】安全性・信頼性の確保

- ブリッジ認証局及び行政機関認証局においては、不正アクセス、災害等への適切なセキュリティ対策を講じる。
- ブリッジ認証局においては、相互認証のための基準を明確に定める。

### 【3】円滑かつ効率的な整備

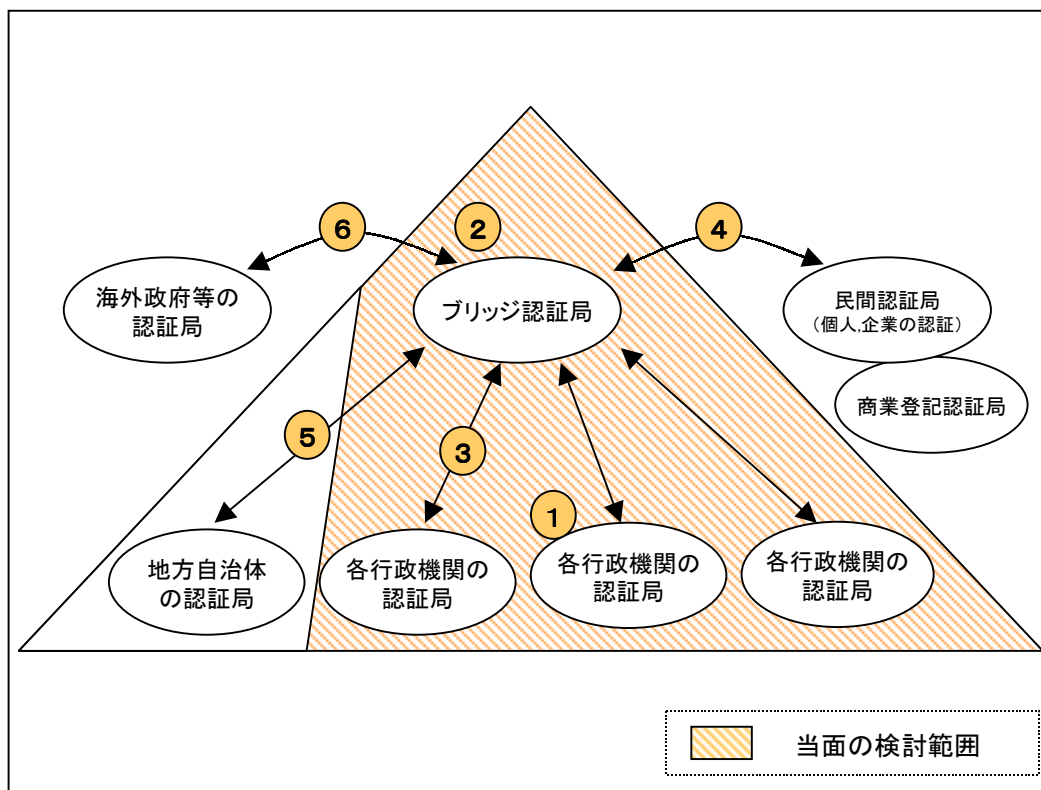
- 行政機関認証局の負担軽減の観点から、全ての行政機関認証局に共通な機能である証明書の有効性検証をブリッジ認証局において実現する。
- ブリッジ認証局の施設を各行政機関で共有できるようにする。

### 【4】拡張性及び汎用性の確保

- 今後における地方公共団体・海外政府等の認証局との相互認証を考慮し、原則として国際的な標準に基づく仕様・技術を採用する。
- 広く利用されている複数の署名アルゴリズムに対応する。

## 政府認証基盤の検討範囲

政府認証基盤及び周囲の認証局との相互認証の位置付けを次のように整理した上で、網掛け部分(①～④)を当面の検討範囲とし、詳細仕様について検討作業を進めてきた。



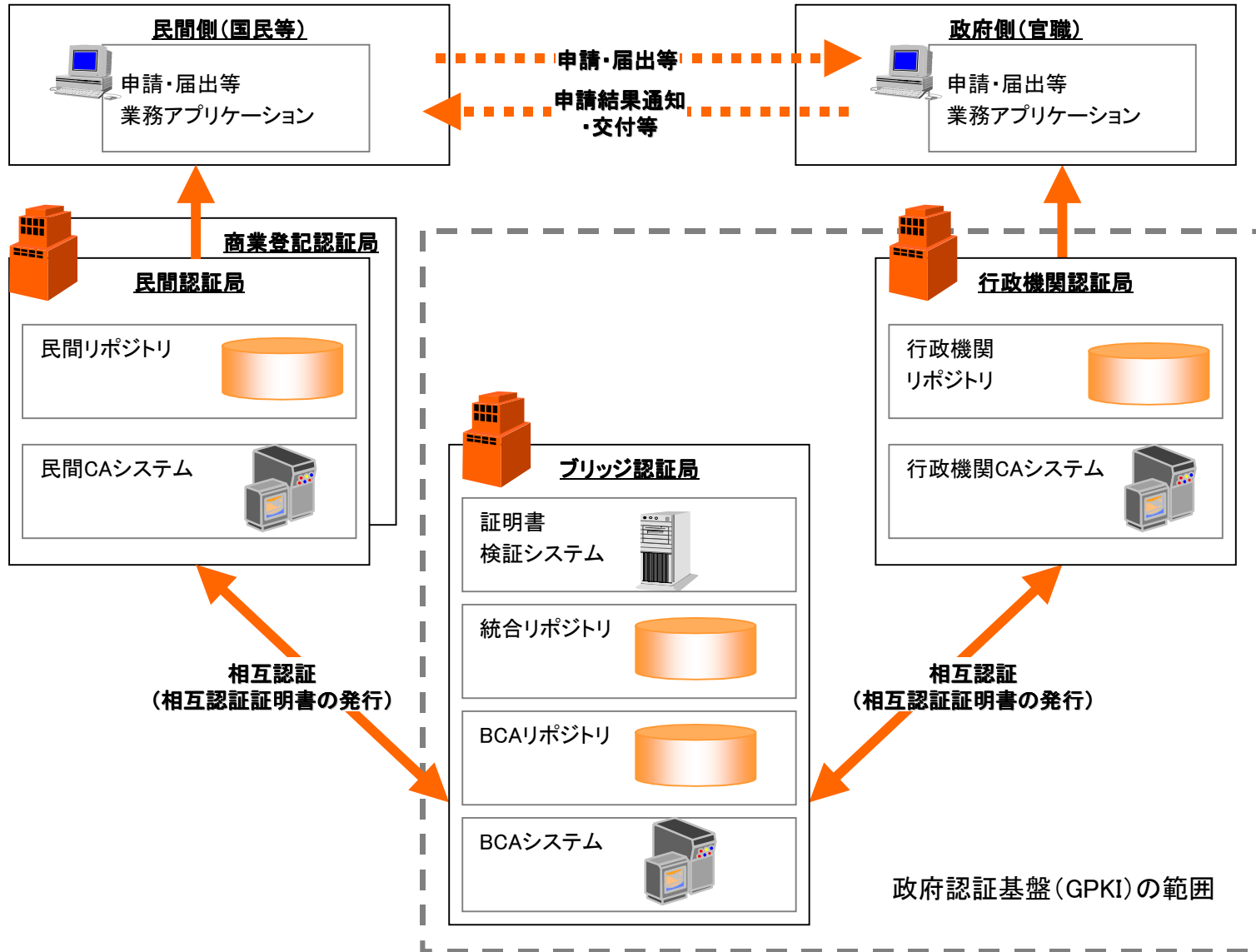
検討対象	詳細仕様の検討内容
① 各行政機関の認証局	<ul style="list-style-type: none"> <li>・システム機能(基本・オプション)の定義</li> <li>・運用方針・手続の定義</li> <li>・施設設備要件・方針の定義</li> <li>・HW・SWの仕様定義</li> </ul>
② ブリッジ認証局	<ul style="list-style-type: none"> <li>・システム機能(基本・拡張)の定義</li> <li>・運用方針・手続の定義</li> <li>・施設設備の定義</li> <li>・HW・SWの仕様定義</li> </ul>
③ ブリッジ認証局と各行政機関の認証局間	<ul style="list-style-type: none"> <li>・相互接続方針の定義</li> <li>・相互接続条件の定義</li> </ul>
④ ブリッジ認証局と民間認証局及び商業登記認証局間	<ul style="list-style-type: none"> <li>・相互接続方針の定義</li> <li>・相互接続条件の定義</li> </ul>

➡ ①から④について、前ページ基本方針を踏まえ、政府認証基盤の基本的在り方、考え方を整理した(第1回フォーラムでの報告内容)。基本的な在り方の整理後、政府認証基盤の詳細仕様について現在検討している。

## 2. 政府認証基盤の詳細仕様の概要

## 政府認証基盤の詳細構成

政府認証基盤は、行政機関認証局とブリッジ認証局により構成される。政府認証基盤を構成するブリッジ認証局と行政機関認証局のシステム構成、及び他システムとの関係を次のように整理した。

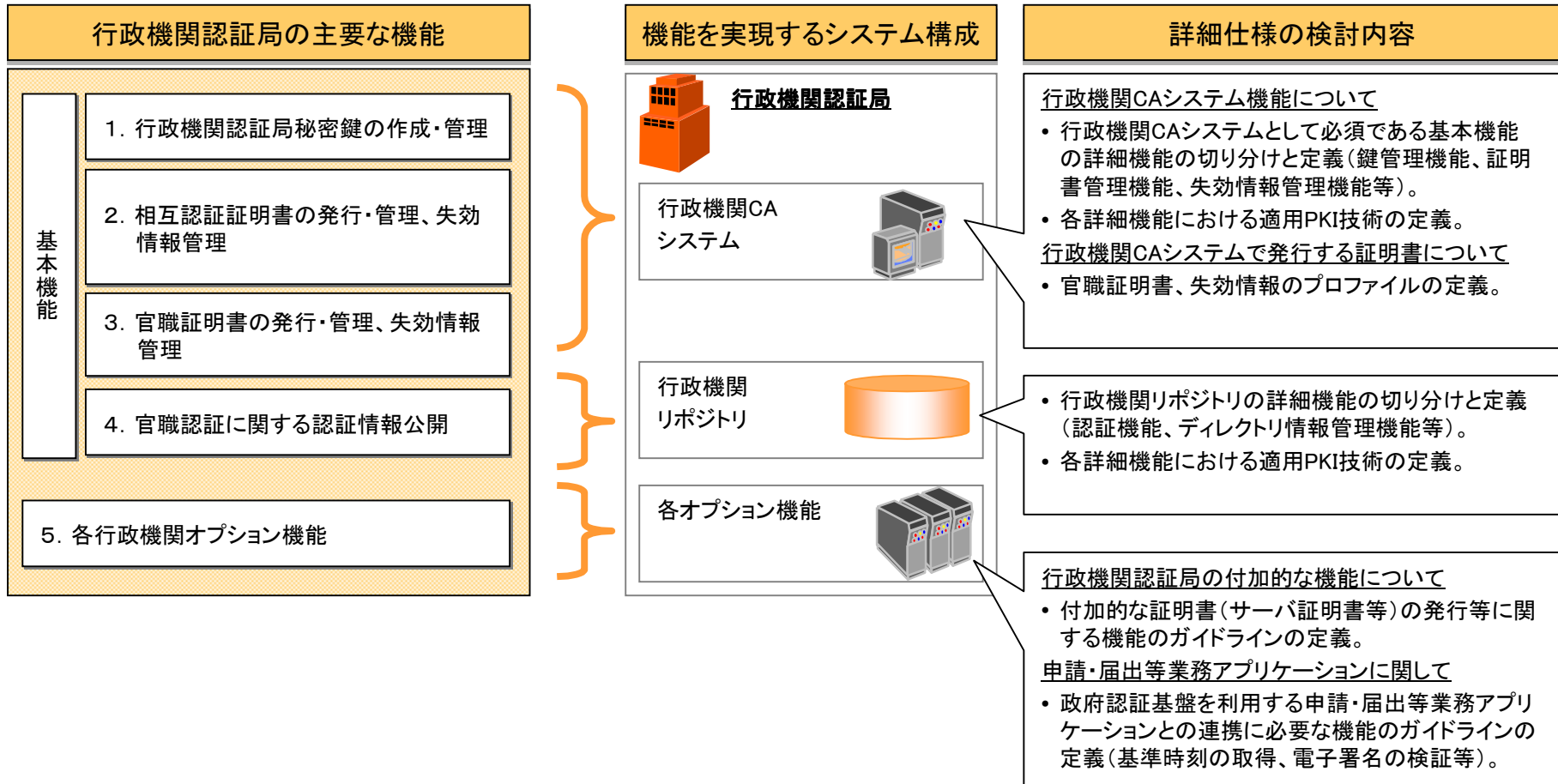


# 行政機関認証局のシステム機能構成

政府認証基盤の基本方針を踏まえて、各行政機関が備えるべき機能の在り方を整理し、各機能を実現するシステム構成の詳細仕様を定義した。前回のフォーラムにおいて提示した行政機関認証局の主要な機能、その機能を実現するためのシステム構成、及び詳細仕様の検討内容は、次のように整理される。

← 前回フォーラムでの提示内容

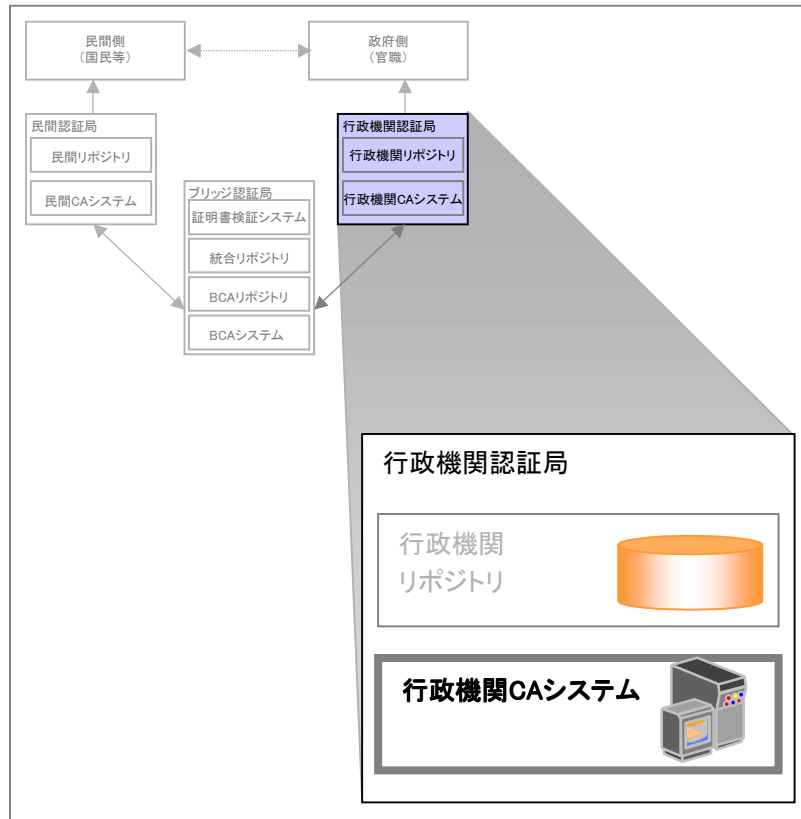
← 今回のフォーラムでの提示内容



## 行政機関認証局のシステム機能－行政機関CAシステム

行政機関CAシステムは官職証明書の発行や失効処理等を行う。行政機関CAシステムの役割と詳細仕様の概要は次のとおりである。

### 行政機関CAシステム



### 役割

- 認証局の公開鍵・秘密鍵ペアを作成し管理する。
- 自己署名証明書の発行、管理を行う。
- 当該機関に属する処分権限者の官職証明書の発行・管理を行う。
- ブリッジ認証局との間で相互認証証明書の発行・失効・更新を行う。
- 認証情報(証明書と失効情報)を行政機関リポジトリに登録する。

### 詳細仕様概要

#### (行政機関CAシステム機能について)

##### 鍵管理機能

- 認証局の秘密鍵は行政機関CAシステムの中でも最重要の機密事項であり外部への漏洩、及び改ざん等の不正アクセスを完全に防止する必要がある。秘密鍵はFIPS140レベル3相当の耐タンパ鍵装置(Hardware Security Module)で管理する。
- 鍵管理機能は鍵生成、鍵廃棄、署名、鍵バックアップを行う。

##### ポリシー管理機能

- 行政機関認証局で発行する証明書及び証明書失効リストのプロファイルの登録・更新・参照をこの機能で実現する。
- 証明書のフォーマットはX.509 v3 証明書フォーマットとする。

##### 証明書発行機能

- 行政機関認証局では、官職証明書、相互認証証明書、自己署名証明書、操作員等の証明書を発行する。
- 省庁の要件によってはサーバ証明書、職員証明書を発行する。(オプション機能)

##### 証明書失効機能

- 発行した証明書の失効、及び証明書失効リスト(CRL、ARL)の発行を行う。

##### 監査ログ機能

- 行政機関CAシステムで監査の対象となる事象(証明書の発行、ポリシーの変更等)が発生した場合に監査記録としてログに記録する。

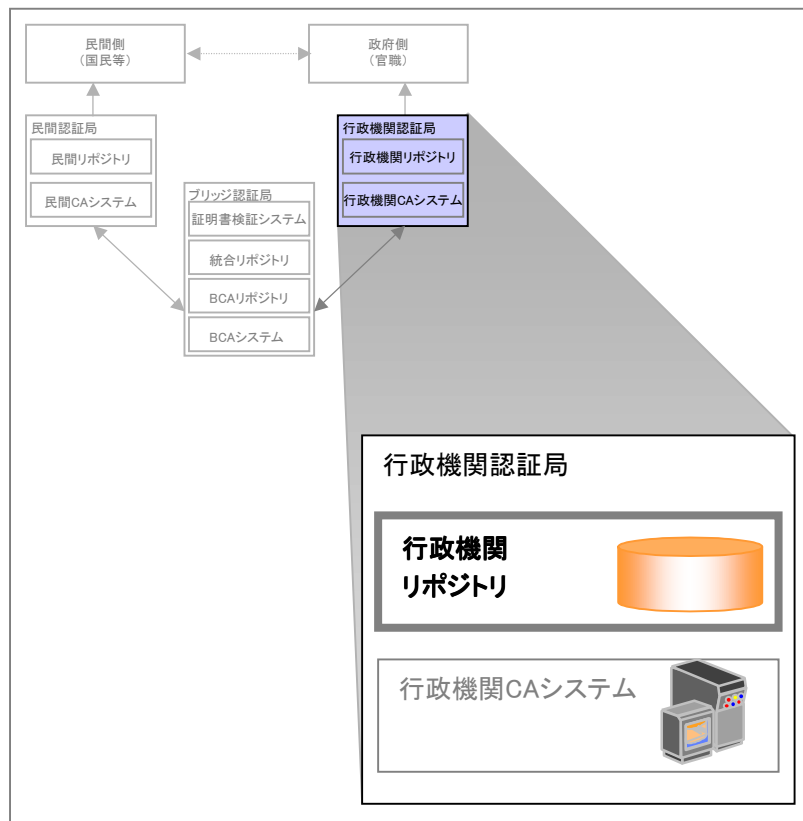
##### バックアップ機能・アーカイブ機能

- 行政機関CA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。
- 行政機関CAシステムが発行した証明書の履歴を管理する。

## 行政機関認証局のシステム機能－行政機関リポジトリ

行政機関リポジトリは行政機関認証局に関する認証情報(証明書や失効情報)の格納・管理を行う。行政機関リポジトリの役割と詳細仕様の概要は次のとおりである。

### 行政機関リポジトリ



### 役割

- 行政機関CAシステムが発行した証明書及び失効情報(認証情報)を格納、管理する。
- 統合リポジトリに対して認証情報を提供する。

### 詳細仕様概要

#### (行政機関リポジトリに格納する情報について)

- 行政機関CAシステムで発行した証明書、失効情報を行政機関リポジトリで管理する。
- 管理する情報は以下の通り
  - 官職認証証明書
  - 相互認証証明書
  - 自己署名証明書
  - 操作員等の認証用の証明書
  - 付加的な証明書(サーバ証明書等)
  - 各証明書の失効情報  
(相互認証証明書・自己署名証明書の各失効情報はARL、他はCRL)

#### (行政機関リポジトリの機能について)

- 行政機関リポジトリを保有し、ブリッジ認証局の統合リポジトリで公開することは基本機能であり、行政機関リポジトリ自身で公開することはオプション機能とする。
- 行政機関リポジトリへのアクセスはLDAPv3により行う。
- 行政機関リポジトリの機能は以下のような機能により構成される。

##### ディレクトリ参照機能

証明書・失効情報への参照リクエストに回答し、認証情報の開示を行う。

##### ディレクトリ更新機能

証明書・失効情報の更新を行う。

##### ログ出力機能

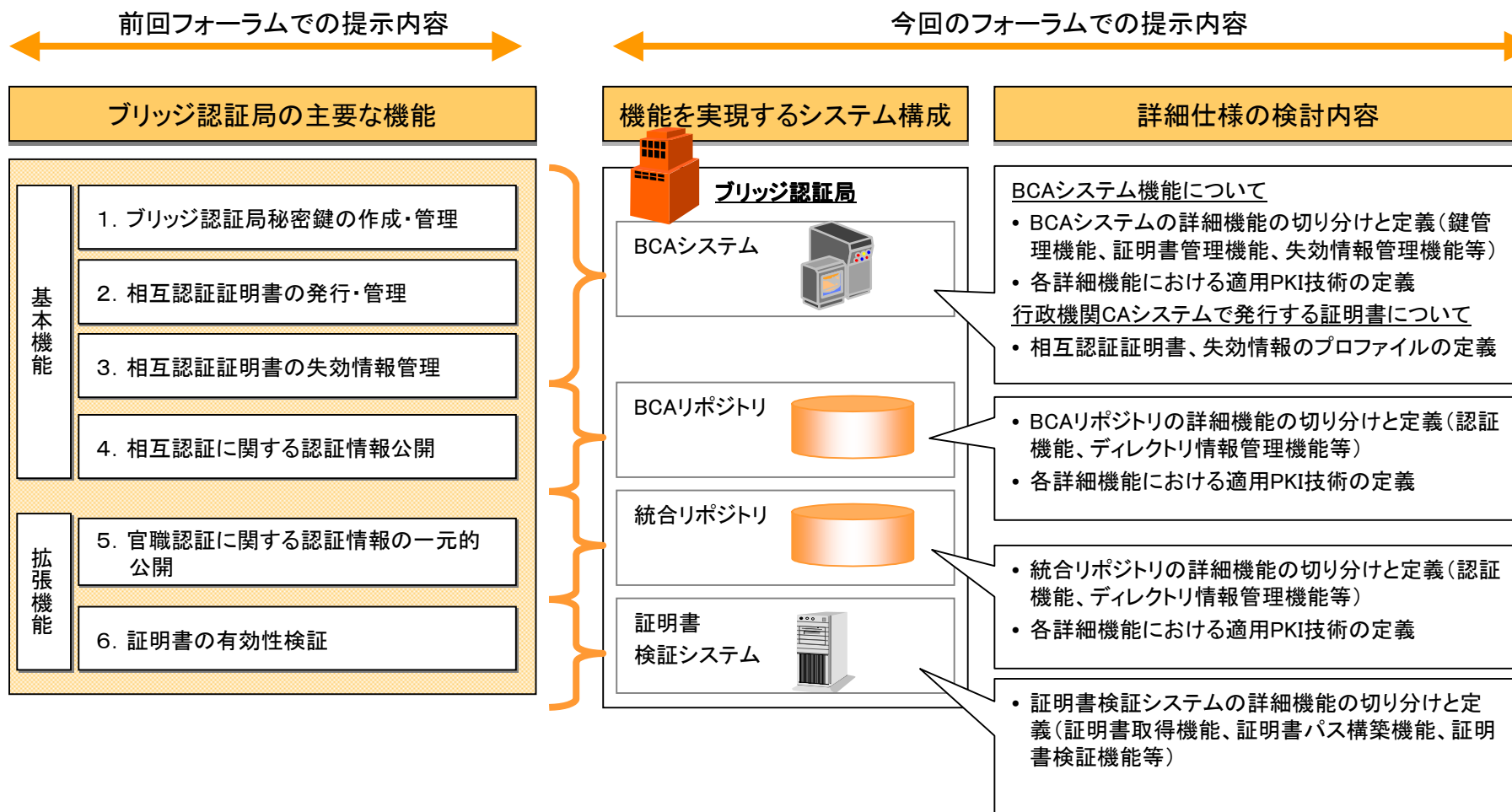
リポジトリに対するリクエスト内容とその結果をログファイルとして外部出力する。

##### バックアップ機能

発行済み証明書、失効情報、その他各種情報を定期的にバックアップする。

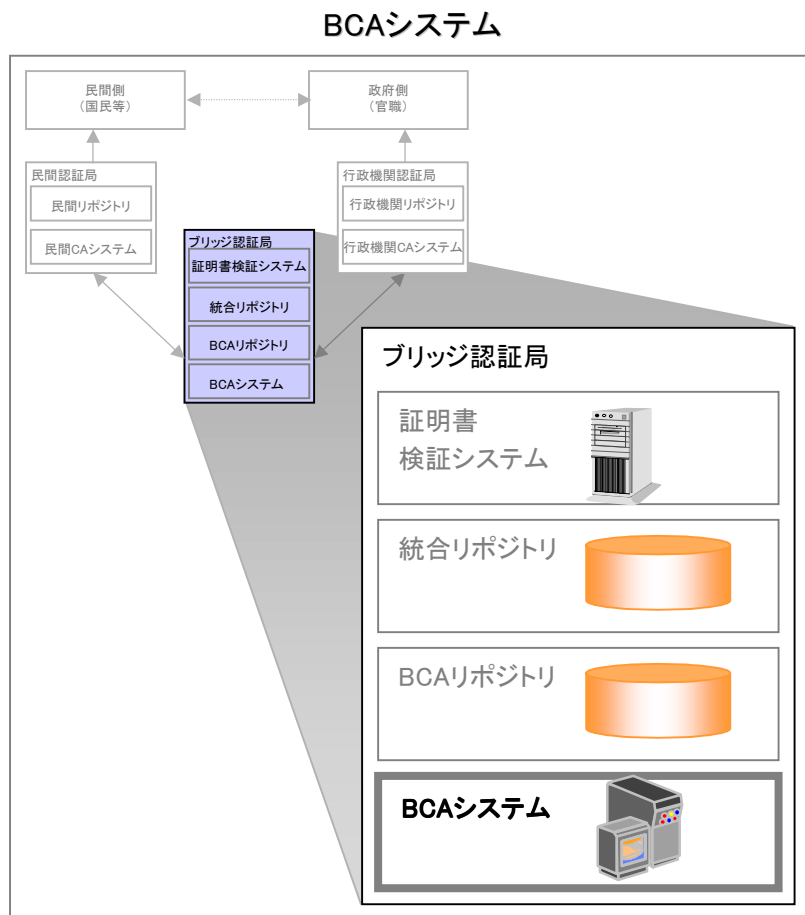
## ブリッジ認証局のシステム機能構成

政府認証基盤の基本方針を踏まえて、ブリッジ認証局が備えるべき機能の在り方を整理し、各機能を実現するシステム構成の詳細仕様を定義した。前回のフォーラムにおいて提示したブリッジ認証局の主要な機能、その機能を実現するためのシステム構成、及び詳細仕様の検討内容は次のように整理される。



## ブリッジ認証局のシステム機能－BCAシステム

BCAシステムは「行政機関認証局」「商業登記に基づく法人認証局」「電子署名法に基づく民間認証局」の各認証局との間で、相互認証証明書及び失効情報の発行を行う。BCAシステムの役割と詳細仕様の概要は次のとおりである。



### 役割

- 認証局の公開鍵・秘密鍵ペアを作成し管理する。
- 自己署名証明書の発行、管理を行う。
- 各認証機関との間で相互認証証明書の発行・失効・更新を行う。
- 認証情報（証明書と失効情報）をBCAリポジトリに登録する。

### 詳細仕様概要

#### (BCAシステム機能について)

##### 鍵管理機能

- 認証局の秘密鍵はBCAシステムの中でも最重要の機密事項であり外部への漏洩、及び改ざん等の不正アクセスを完全に防止する必要がある。秘密鍵はFIPS140レベル3相当の耐タンパ鍵装置 (Hardware Security Module) で管理する。
- 鍵管理機能は鍵生成、鍵廃棄、署名、鍵バックアップを行う。

##### ポリシー管理機能

- ブリッジ認証局で発行する証明書及び証明書失効リストのプロファイルの登録・更新・参照をこの機能で実現する。
- 証明書のフォーマットはX.509 v3 証明書フォーマットとする。

##### 証明書発行機能

- ブリッジ認証局では、相互認証証明書、自己署名証明書、操作員等の証明書を発行する。この機能により、証明書の発行要求を受付、証明書を作成する。
- 各認証局との相互認証はオフラインで実施し、証明書要求はPKCS#10のフォーマットで可搬媒体で受け付ける。
- 証明書発行機能は、証明書発行要求受付、証明書発行、証明書発行要求生成、証明書出力により構成される。

##### 証明書失効機能

- 発行した証明書の失効、及び証明書失効リスト (CRL、ARL) の発行を行う。
- 証明書失効要求受付、証明書ステータス変更、証明書失効リスト出力機能から構成される。

##### 監査ログ機能

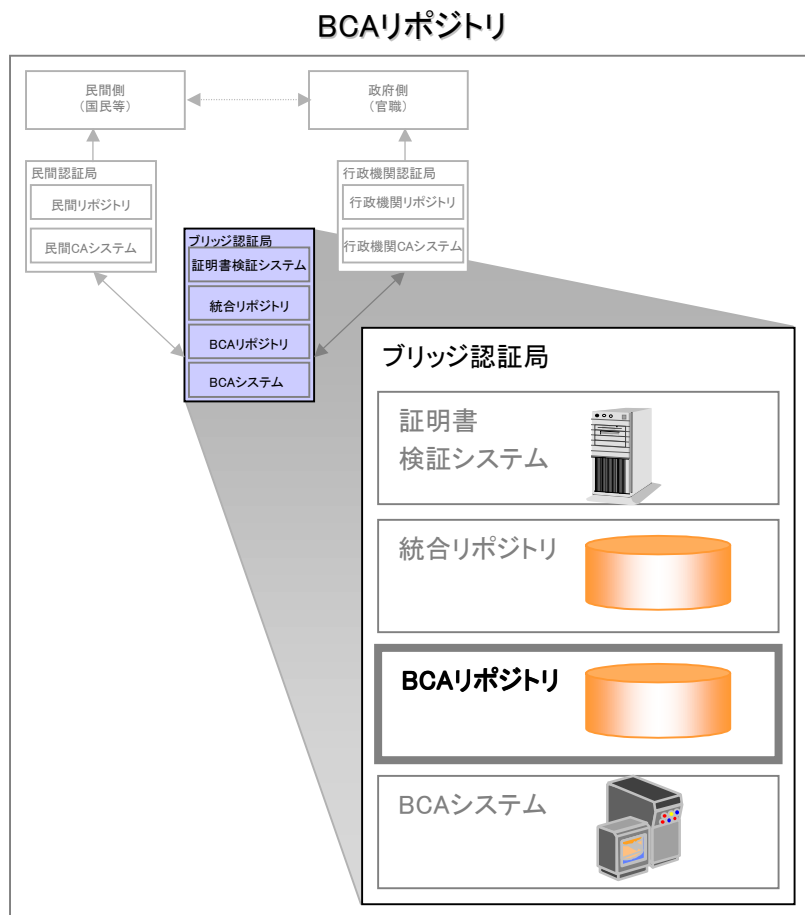
- BCAシステムで監査の対象となる事象（証明書の発行、ポリシーの変更等）が発生した場合に監査記録としてログに記録する。

##### バックアップ機能・アーカイブ機能

- BCA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。
- BCAシステムが発行した証明書の履歴を管理する。

## ブリッジ認証局のシステム機能－BCAリポジトリ

BCAリポジトリはブリッジ認証局が発行した自己署名証明書、相互認証証明書、失効情報の登録、保管のための機能を提供する。BCAリポジトリの役割と詳細仕様の概要は次のとおりである。



### 役割

- BCAシステムが発行した証明書及び失効情報(認証情報)を格納、管理する。
- 統合リポジトリに対して認証情報を提供する。

### 詳細仕様概要

#### (BCAリポジトリに格納する情報について)

- BCAシステムで発行した証明書、失効情報をBCAリポジトリで管理する。
- 管理する情報は以下の通り
  - 相互認証証明書
  - 自己署名証明書
  - 操作員等の認証用の証明書
  - 相互認証証明書失効情報(ARL)
  - 自己署名証明書失効情報(ARL)
  - 操作員等の認証用の証明書失効情報

#### (BCAリポジトリの機能について)

- BCAシステムが発行した認証情報を格納する。
- BCAリポジトリへのアクセスはLDAPv3により行う。
- BCAリポジトリの機能は以下のような機能により構成される。

##### ディレクトリ参照機能

証明書・失効情報への参照リクエストに回答し、認証情報の開示を行う。

##### ディレクトリ更新機能

証明書・失効情報の更新を行う。

##### ログ出力機能

リポジトリに対するリクエスト内容とその結果をログファイルとして外部出力する。

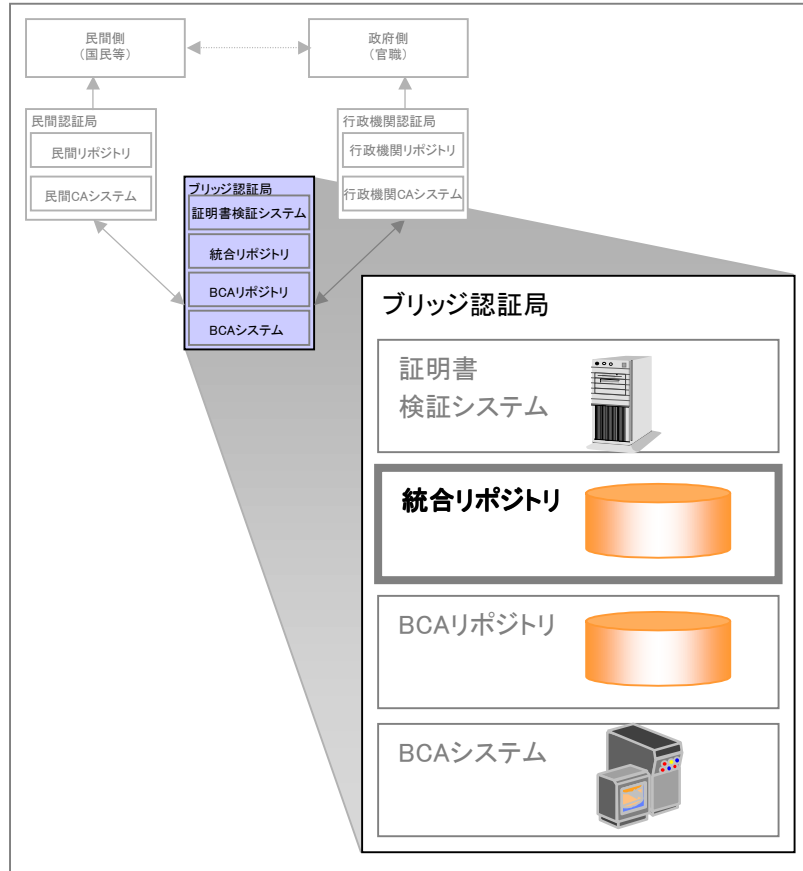
##### バックアップ機能

発行済み証明書、失効情報、その他各種情報を定期的にバックアップする。

# ブリッジ認証局のシステム機能－統合リポジトリ

統合リポジトリはブリッジ認証局と行政機関認証局が発行した証明書及び失効情報を公開するための機能を提供する。統合リポジトリの役割と詳細仕様の概要は次のとおりである。

## 統合リポジトリ



## 役割

- BCAシステムが発行した証明書・失効情報（認証情報）を格納、公開する。
- 各行政機関CAシステムが発行した認証情報を格納する。
- 申請・届出等業務アプリケーションや証明書検証システムに認証情報を提供する。

## 詳細仕様概要

### （統合リポジトリの特徴と格納する情報について）

- 統合リポジトリは、国民等に対する効率的な認証情報の提供と各省庁の負担軽減の観点から、統合的に認証情報の公開・管理する。
- 以下のような認証情報を一元的に提供する。

#### （ブリッジ認証局が発行した認証情報）

- 相互認証証明書
- 自己署名証明書
- 各証明書の失効情報

#### （行政機関認証局が発行した認証情報）

- 相互認証証明書
- 自己署名証明書
- 官職証明書
- 各証明書の失効情報

#### （民間認証局が発行した認証情報の所在情報）

- 認証情報そのものは格納しないがLDAPv3による参照連携（リフェラル連携）により情報提供を行う。

### （統合リポジトリの機能について）

- 統合リポジトリへのアクセスは、LDAPv3により行う。
- 統合リポジトリはBCAリポジトリと同様に以下のような機能により構成される。

#### ディレクトリ参照機能

証明書・失効情報への参照リクエストに回答し、認証情報の開示を行う。

#### ディレクトリ更新機能

証明書・失効情報の更新を行う。

#### ログ出力機能

統合リポジトリに対するリクエスト内容とその結果をログファイルとして外部出力する。

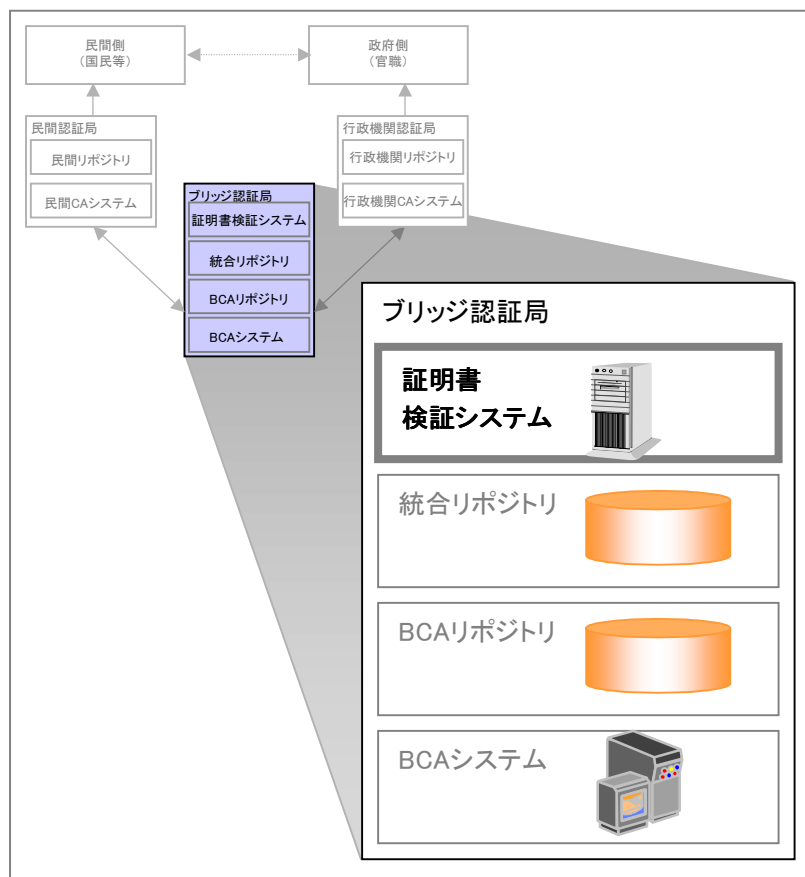
#### バックアップ機能

発行済み証明書、失効情報、その他各種情報を定期的にバックアップする。

## ブリッジ認証局のシステム機能－証明書検証システム

証明書検証システムは各省庁向けの拡張機能として認証パス構築及び証明書有効性検証を代理する機能をもつ。証明書検証システムの役割と詳細仕様の概要は次のとおりである。

### 証明書検証システム



### 役割

- 証明書検証システムは申請・届出等業務アプリケーションの機能に代わり、証明書の有効性の検証を代理で実施する。
- 証明書の認証パスの構築、証明書の有効性の確認を実施する。

### 詳細仕様概要

#### (証明書検証システムの特徴について)

- 相互認証が広範に広まった場合に、証明書検証の複雑化に対応するために、各省庁の負担軽減を目的としている。
- 政府側申請・届出等業務アプリケーションに代わって、相互認証証明書や各個別の証明書や各失効情報(CRL、OCSP)を取得し、証明書の有効性を検証する。
- 政府側申請・届出等業務アプリケーションと証明書検証システムとの通信はOCSP+拡張を採用。
- 統合リポジトリにアクセスして各認証情報を取得する。

#### (証明書検証システムの機能について)

##### 証明書取得機能

- 認証パスの構築に必要な証明書を統合リポジトリや民間認証局からLDAPv3プロトコルを使用して取得する。

##### CRL/ARL取得機能

- 証明書取得機能で取得した証明書のCRL/ARLを、統合リポジトリや民間CAからLDAPv3プロトコルを用いて取得する。

##### OCSPクライアント機能

- 証明書の失効情報をOCSPで提供している認証局に対して、証明書の検証依頼をOCSPで依頼する。

##### 認証パス構築機能

- 証明書検証システムへの要求に応じた認証パスの構築を行う。

##### 署名検証機能

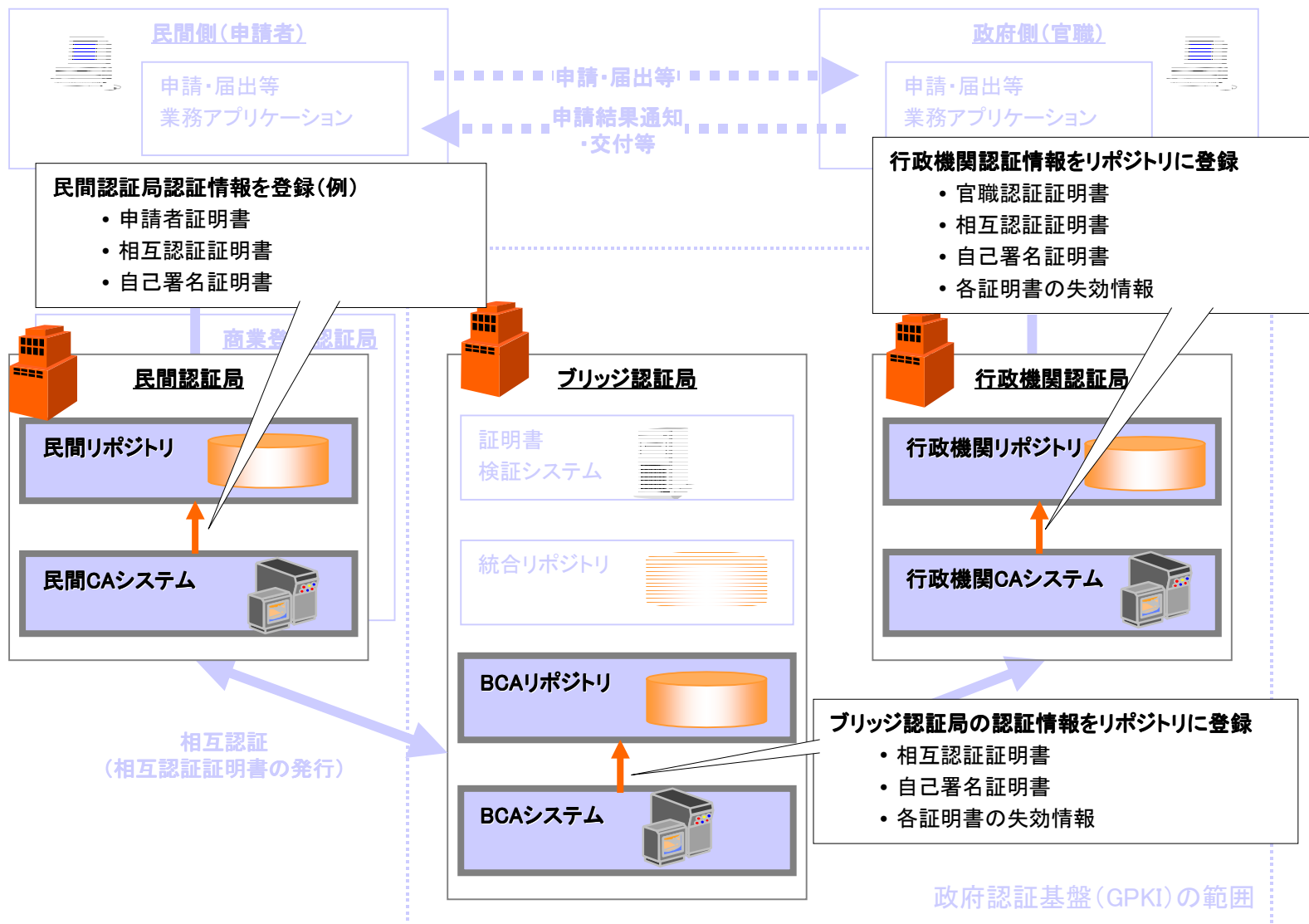
- 次の署名に対して証明書による検証を行い、署名検証結果を生成する。
  - 認証パスの各証明書発行者の署名
  - CRL/ARL発行者の署名
  - OCSP応答者の署名

##### 有効性検証機能

- 構築された認証パスの有効性の検証をCRL/ARLやOCSP応答情報を使用して行う。

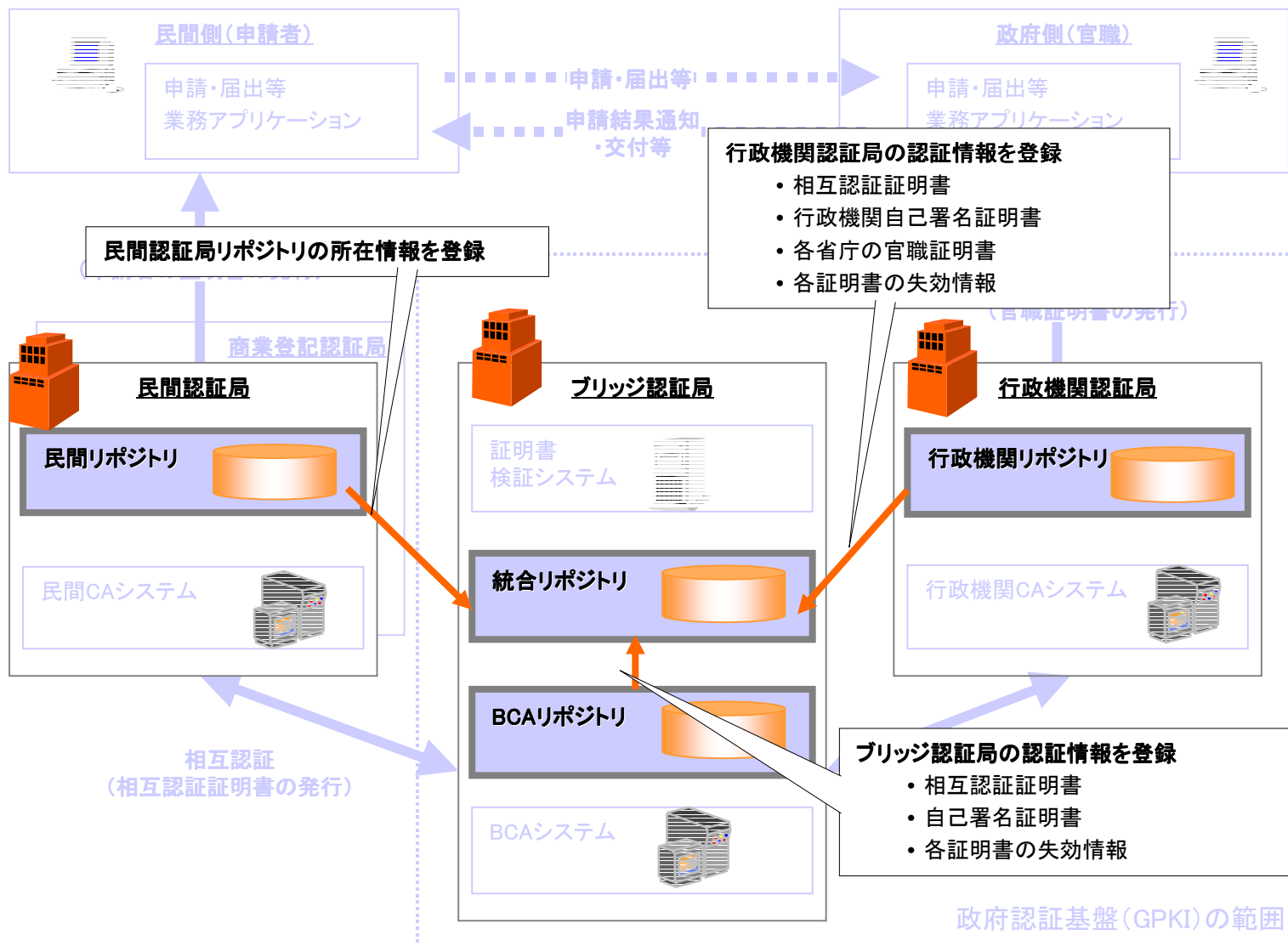
## 各システム構成要素の連携－各リポジトリへの認証情報の登録

これまで説明を行ってきた各システム構成要素の連携関係について整理する。各CAシステムとリポジトリ間の連携は、次のように整理される。



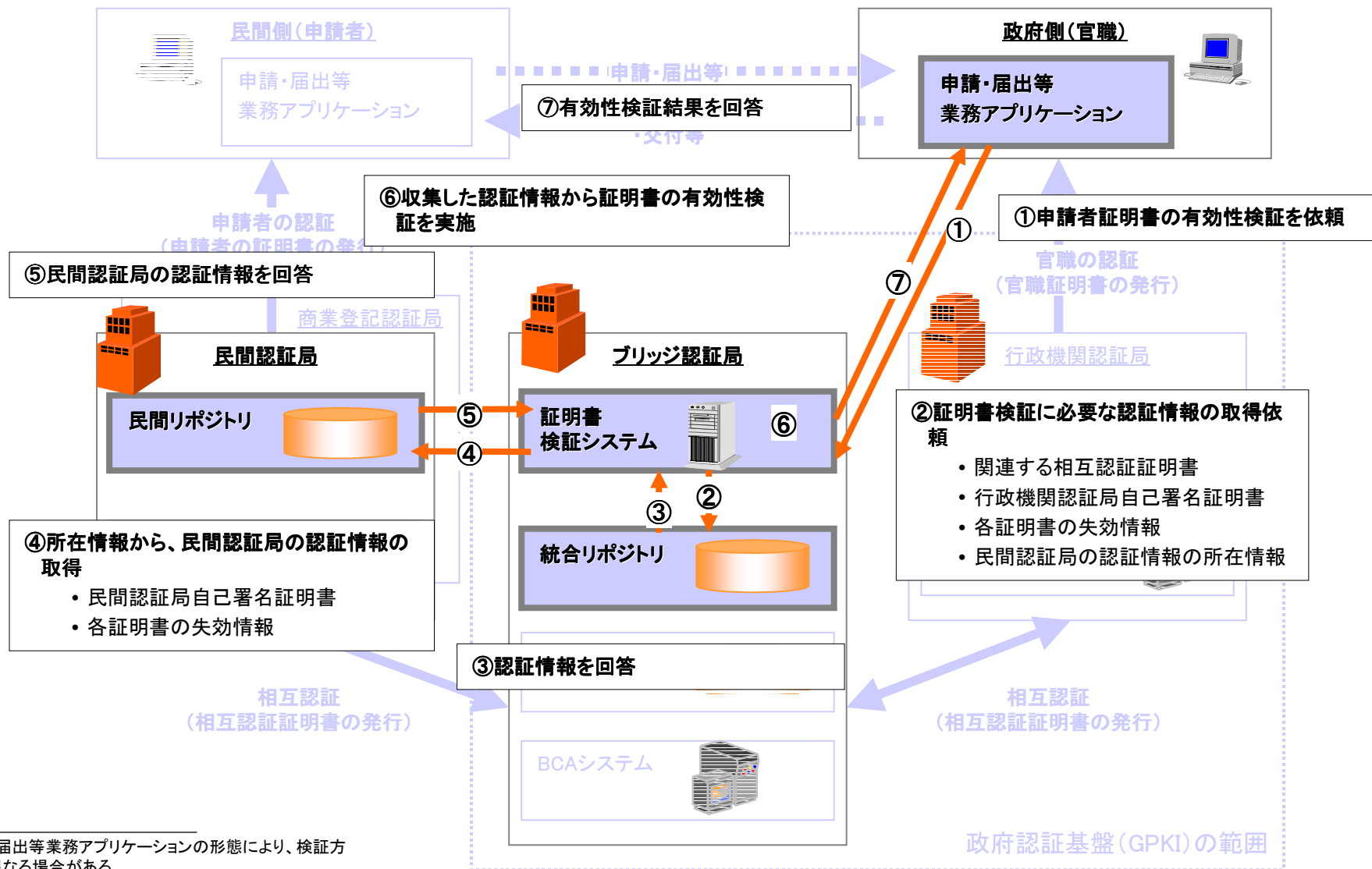
## 各システム構成要素の連携－統合リポジトリへの認証情報の登録

各認証局のリポジトリと統合リポジトリの連携は、次のように整理される。



## 各システム構成要素の連携－申請者証明書の有効性検証

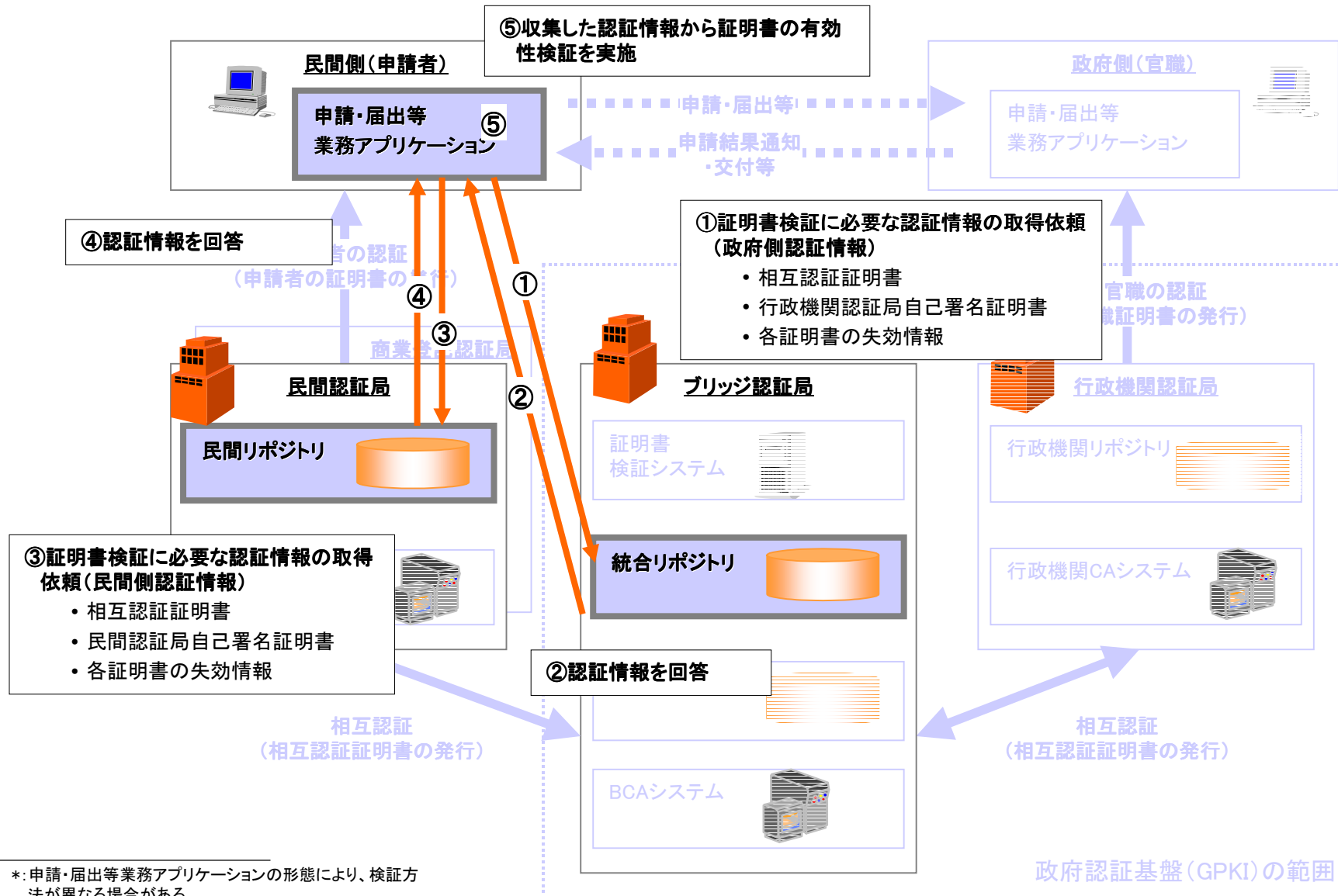
申請者証明書の有効性を検証する際の各システム構成要素の連携は、次のように整理される。(\*)



\*: 申請・届出等業務アプリケーションの形態により、検証方法が異なる場合がある。  
ここでは、一例として説明を行う。

## 各システム構成要素の連携－官職証明書の有効性検証

官職証明書の有効性を検証する際の各システム構成要素の連携は、次のように整理される。(\*)



\*: 申請・届出等業務アプリケーションの形態により、検証方法が異なる場合がある。  
ここでは、一例として説明を行う。

## 政府認証基盤運用方針・運用手続

政府認証基盤を運営するにあたり、行政機関認証局とブリッジ認証局の運営方針・運用手続について検討した。

### 行政機関認証局

#### 検討の内容

- 運用方針について
  - 行政機関認証局の運営に関して、運営組織、危機管理、監査等の事項について最低限必要となる方針を定義。
- 運用手続について
  - 行政機関認証局の運営に関する手続について、最低限必要となる運用手続を洗い出し、要件を整理。

#### 運営方針

- 運営組織
  - 行政機関認証局に必要な組織(ポリシー委員会、センター運用組織等)を識別しその役割、権限を定義
- 危機管理
  - 不正アクセス、災害等で行政機関認証局の秘密鍵が危殆化した場合等の管理方針を定義
- 監査
  - 行政機関認証局の信頼性を保つために必要な監査について、監査の体制や実施方針について定義

#### 手続

- 証明書関連業務
  - 官職証明書発行、管理手続
  - 官職証明書の失効手続
  - 相互認証証明書の発行、管理手続
  - 相互認証証明書の失効手続
- 等

### ブリッジ認証局

#### 検討の内容

- 運用方針について
  - ブリッジ認証局の運営に関して、運営組織、危機管理、監査等の事項について必要となる方針を定義。
- 運用手続について
  - ブリッジ認証局の運営に関する手続について、必要となる運用手続を洗い出し、要件を整理。

#### 運営方針

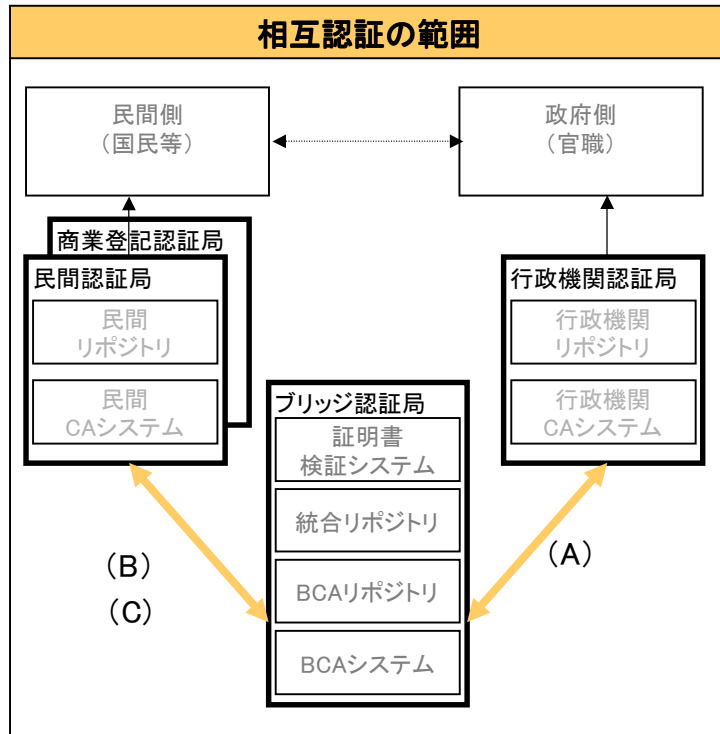
- 運営組織
  - ブリッジ認証局に必要な組織(ポリシー委員会、センター運用組織等)を識別しその役割、権限を定義
- 危機管理
  - 不正アクセス、災害等でブリッジ認証局の秘密鍵が危殆化した場合の管理方針を定義
- 監査
  - 政府認証基盤の信頼性を保つために必要な監査について、監査の体制や実施方針について定義

#### 手続

- 証明書関連業務
  - 相互認証証明書の発行、管理手続
  - 相互認証証明書の失効手続
- 等

## 政府認証基盤相互認証接続条件－全体概要

(A)各行政機関認証局との相互認証、(B)民間認証局との相互認証、及び(C)商業登記認証局との相互認証に関する相互認証方針及び接続条件は次のとおりである。



### 詳細仕様検討の内容

#### (A) 行政機関認証局との相互認証について

##### ・相互認証方針

- 行政機関認証局は、ブリッジ認証局とのみ相互認証を行い、民間認証局と直接相互認証を行わない。また、行政機関認証局においては、最上位の認証局と下位の認証局間での相互認証は行わない。
- ブリッジ認証局は、行政機関認証局の最上位の認証局とのみ相互認証を行う。

##### ・相互認証接続条件

- 政府認証基盤としての整合性を確保するため、各行政機関認証局が満たすべき、最低限の基準を設定する。この接続条件について詳細仕様を定義した。次ページ以降に記述する。

#### (B) 民間認証局との相互認証について

##### ・相互認証方針

- ブリッジ認証局は、電子署名及び認証業務に関する法律に基づく認定を受けた民間認証局とのみ相互認証を行う。

##### ・相互認証接続条件

- 相互認証基準の内容は、電子署名及び認証業務に関する法律に基づく認定基準に加え、政府認証基盤として必要な接続基準を付加したものとする。次ページ以降に接続条件について記述する。

#### (C) 商業登記認証局との相互認証について

- 商業登記認証局の機能や証明書等について詳細に調整を行い、具体的な接続方法について検討。

## 政府認証基盤相互認証接続条件ーブリッジ認証局と行政機関認証局との接続条件

ブリッジ認証局と行政機関認証局との接続条件は、官職認証に関する接続条件と相互認証に関する接続条件の両者を満たすことが必要となる。

### ブリッジ認証局への行政機関認証局接続条件

システム機能面

#### 官職認証に関する行政機関認証局の接続条件

官職認証に関して、政府認証基盤全体の信頼性を確保可能な最低限のシステム機能を保有すること。

- 認証局や官職の秘密鍵が一定の条件を満たした方式で管理されていること。
  - 官職証明書が一定の条件を満たした署名アルゴリズム及び鍵長を使用できること。
- 等

#### 相互認証に関する行政機関認証局接続条件

相互認証に最低限必要であり、政府認証基盤全体の信頼性を確保するシステム機能を保有すること。

- 相互認証証明書の発行要求機能
  - 相互認証証明書の発行機能
  - 相互認証証明書の失効機能
  - 相互認証証明書を公開するリポジトリ機能
  - 一定の条件を満たした署名アルゴリズム及び鍵長を使用できること。
- 等

指定された相互認証証明書を作成できること。

- 指定された相互認証証明書プロファイルで発行できること。
- 等

運用手続面

#### 官職認証に関する行政機関認証局の接続条件

官職認証に関して、政府認証基盤全体の信頼性を確保可能な最低限の運用方針・手続が定義されていること。

- 監査手続
  - 緊急時の対応・手続
- 等

#### 相互認証に関する行政機関認証局接続条件

相互認証に最低限必要であり、政府認証基盤全体の信頼性を確保する運用方針・手続が定義されていること。

- 相互証明書の発行手続、失効手続
  - 監査手続
  - 緊急時の対応手続
- 等

施設設備面

#### 官職認証に関する行政機関認証局の接続条件

政府認証基盤全体の信頼性を確保可能な施設設備を保有すること。

- 入退室管理・室内監視のための設備
  - セキュリティ室の設置
- 等

## 政府認証基盤相互認証接続条件－民間認証局の政府認証基盤接続条件

民間認証局の政府認証基盤接続条件は、「電子署名及び認証業務に関する法律」に基づく認定基準を満たし、かつ政府認証基盤に接続する条件として政府認証基盤のブリッジ認証局に相互認証するための要件も満たすこととする。なお、「電子署名及び認証業務に関する法律」に基づく認定基準は、省令で定められる予定となっている。

### 政府認証基盤への民間認証局接続条件 =

#### “電子署名及び認証業務に関する法律”に基づく認定

- 電子署名及び認証業務に関する法律で省令の定めるべき基準で認定されている民間認証局とブリッジ認証局は相互接続を行う。

##### 設備基準(第6条1項1)

認定認証業務を実施するにあたり必要となる設備面での条件。

##### 本人確認方法(第6条1項2)

認定認証業務を実施するにあたり必要となる本人確認方法についての条件。

##### その他の基準(第6条1項3)

認定認証業務を実施するにあたり必要となるその他の条件。

+

#### 相互認証に関する民間認証局接続条件

- 電子署名及び認証業務に関する法律に基づく認定に加え以下のような条件を満たすことが相互接続を実施する上で必要となる。

システム機能面

相互認証に最低限必要であり、政府認証基盤全体の信頼性を確保するシステム機能を保有すること。

- 相互認証証明書の発行要求機能
- 相互認証証明書の発行機能
- 相互認証証明書の失効機能
- 相互認証証明書を公開するリポジトリ機能
- 一定の条件を満たした署名アルゴリズム及び鍵長を使用できること。

等

指定された相互認証証明書を作成できること。

- 指定された相互認証証明書プロファイルで発行できること。

等

運用手続面

相互認証に最低限必要であり、政府認証基盤全体の信頼性を確保する運用方針・手続が定義されていること。

- 相互証明書の発行手続、失効手続
- 監査手続
- 緊急時の対応手続

等



電子署名及び認証業務に関する法律で省令の定める基準が明確になり次第、政府認証基盤への接続条件を見直していく。

## 政府認証基盤 施設設備/HW・SWの必要要件

政府認証基盤を構成する施設設備及びHW・SWについて、安全性・信頼性の確保の観点を中心として必要となる要件・仕様を検討した。

### 行政機関認証局

#### 検討の内容

- 施設設備について
  - 行政機関認証局のセンター施設設備について、最低限必要な設備施設要件について定義。
- HW・SWについて
  - 行政機関認証局のシステム機能を実現するために最低限必要となるHW・SWの構成、仕様を定義。

#### 施設設備

- 建物
  - 行政機関認証局及び関連施設に関して、建物の設置要件、場所等の要件について整理。
- 空調設備
  - 行政機関認証局の空調設備について設置要件、設備仕様についての要件を整理。
- 電気設備
  - 行政機関認証局の電源設備について、電力供給の仕様、災害対策等の要件について整理。
- 防災・防犯設備
  - 行政機関認証局に関して防災・防犯上必要となる設備について、壁構造仕様、監視カメラ仕様、入退室管理仕様についての要件を整理。

#### HW・SW

- 行政機関認証局のシステム機能を実現するためのHW・SWについてセキュリティ対策、可用性、信頼性を考慮し必要となる構成、仕様を定義。

### ブリッジ認証局

#### 検討の内容

- 施設設備について
  - ブリッジ認証局のセンター施設設備について、必要な設備施設要件について定義。
- HW・SWについて
  - ブリッジ認証局のシステム機能を実現するための必要最低限となるHW・SWの構成、仕様を定義。

#### 施設設備

- 建物
  - ブリッジ認証局及び関連施設に関して、建物の設置要件、場所等の要件について整理。
- 空調設備
  - ブリッジ認証局の空調設備について設置要件、設備仕様についての要件を整理。
- 電気設備
  - ブリッジ認証局の電源設備について、電力供給の仕様、災害対策等の要件について整理。
- 防災・防犯設備
  - ブリッジ認証局に関して防災・防犯上必要となる設備について、壁構造仕様、監視カメラ仕様、入退室管理仕様についての要件を整理。

#### HW・SW

- ブリッジ認証局のシステム機能を実現するためのHW・SWについてセキュリティ対策、可用性、信頼性を考慮し必要となる構成、仕様を定義。