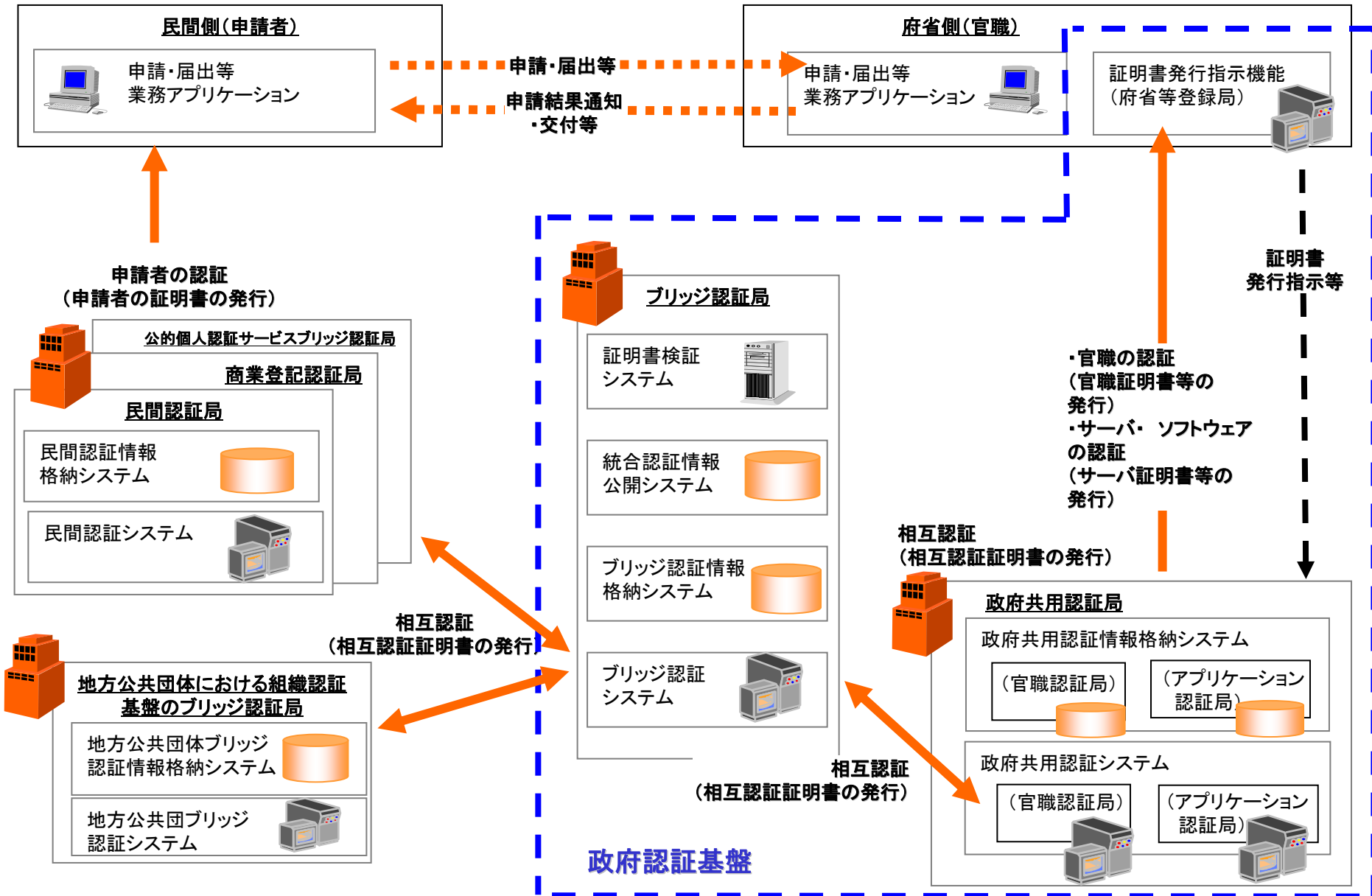

政府認証基盤の基本的な仕様

参考資料

政府認証基盤のシステム構成図



【アルファベット順】

FIPS140-1、FIPS140-2(Federal Information Processing Standard)

NIST(米国標準技術研究所)が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。コンピュータと通信システムの暗号モジュールに対して暗号技術に関する汎用要件を網羅しており、最低レベル1から最高レベル4までのセキュリティレベルが設定されている。FIPS140-1は、1994年1月11日に発行されたが、その後改定され2001年5月25日にFIPS140-2が発行された。

- レベル1: FIPSで定義している最低限のセキュリティレベルであり、物理的なセキュリティ手段までは必要ないレベル。一般的なPCに適用されているような暗号モジュールに適用されている。
- レベル2: レベル1の要件に物理的セキュリティ(コーティングやシール、こじ開け防止ロック)を加え、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えているレベル。また、役割ベースの認証が付与されている。
- レベル3: レベル2の要件の物理的セキュリティを強化したもので、暗号モジュールへのアクセスを検出し暗号鍵やパスワード等重要なパラメータへの不正アクセスを防止できるレベル。また、レベル2より安全性の高いユーザ認証を実装している。暗号鍵やパスワード等重要なパラメータに不正アクセスしようとした場合には、重要なパラメータをすべて消去するような仕組みを持つものもある。
- レベル4: FIPSで定義している最高レベルのセキュリティレベルであり、レベル3をさらに強化したものである。すべての物理的な不正アクセスを検知する機能を持ち、暗号鍵やパスワード等重要なパラメータへ不正アクセスしようとした場合には、重要なパラメータをすべて消去する仕組みを持つ。また、温度の変化や電流の変化等の環境の変動も検知できるような仕組みを導入しているレベル。

LDAP(Lightweight Directory Access Protocol)

電子メールアドレスを検索するディレクトリサービスのために作られたプロトコル。通信形式はクライアント・サーバ型を採用している。Version3(v3)では、サーバ間でのディレクトリ情報のコピー機能やセキュリティ機能が強化されている。

OCSP(Online Certificate Status Protocol)

現在の証明書の状態(失効していないかどうか)をオンラインで問い合わせるプロトコル。クライアントは、OCSPのサーバに対して、調べるべき証明書のシリアル番号を指定して、署名を付けて問い合わせる。OCSPサーバは、問い合わせのあった証明書が失効しているかないかの状態をOCSPサーバの署名を付けて返す。このOCSPサーバは信頼できる認証局の認証を受けたものである必要がある。

PKCS(Public Key Cryptography Standards)#10

PKCSは、米国RSA Data Security社による公開鍵暗号方式を実現するための技術。米国のNetscape社やMicrosoft社など多数の会社にライセンスされている。PKCS #10は、認証局に対する証明書発行要求メッセージの構文(Certification Request Syntax Standard)に関する規格。

RFC2527(Request For Comments 2527)

インターネットを推進する規範を示す標準文書の一つ。RFC2527は、認証局や公開鍵インフラストラクチャのための認証ポリシーもしくは認証実施規程を作成するためのフレームワークやガイドラインを提供している。

RFC3647(Request For Comments 3647)

インターネットを推進する規範を示す標準文書の一つ。RFC2527をPKI運用の技術的要素及び法的要素を考慮し、更新したもの。

UCS(Universal multiple-octet coded Character Set)

世界中の主要な文字を一括して扱う多重言語文字セット規格。国際標準化機構(ISO)により制定された。文字セットはどの文字を扱うかを定める規格を指す。

UTF-8(8-bit UCS Transformation Format) String

UCSで定義された文字セットをバイト列によって表現する文字コードの一つ。他にUTF-16がある。

X.509

ITU-T(国際電気通信連合-電気通信標準化部門)が定めた公開鍵証明書及び証明書失効リストのフォーマット。X.509 v3(Version 3)では、任意の情報を埋め込むための拡張方式が前バージョンより追加された。政府認証基盤では公開鍵証明書はX.509 v3、証明書失効リストはX.509 v2を使用する。

用語解説(2/3)

【カ行】

公開鍵

公開鍵暗号方式において用いられる公開されている鍵のこと。

公開鍵暗号方式

暗号時と復号時にそれぞれ異なる鍵ペア(公開鍵と秘密鍵)を用いる暗号方式。代表的なものにRSA暗号がある。また、この原理を応用して署名時に秘密鍵、署名検証時に公開鍵を用いることにより電子署名の仕組みを実現することができる。

コード署名証明書

インターネットを利用して、ソフトウェアを安全に配布するために用いる公開鍵証明書。コード署名証明書により配布元をなりすましたり、プログラムが改竄されていないことを保証することができる。

【サ行】

サーバ証明書

クライアント、サーバ間で安全な通信を行うために、そのサーバが信頼できるものであることを証明した公開鍵証明書。

自己署名証明書

自己の公開鍵に対して、自己の秘密鍵で署名した公開鍵証明書。

失効情報

証明書の有効期間中に証明書の内容を変更した場合や秘密鍵の盗難、紛失、破壊などが生じた場合、認証局が提供する証明書の失効を示す情報。

証明書失効リスト

証明書の有効期間中に証明書の内容変更、秘密鍵の盗難、紛失、破壊などが生じたため失効した証明書のリスト。失効リストには、失効対象の証明書を発行した認証局の署名が付与される。官職証明書・申請者証明書の失効リストをCRL(Certificate Revocation List)、自己署名証明書・相互認証証明書の失効リストをARL(Authority Revocation List)という。

署名アルゴリズム

公開鍵暗号方式を利用した署名のアルゴリズム。RSA、DSA等の方式がある。

相互認証証明書

2つの異なる認証ドメインの認証局がお互いの条件を充足して相互認証したことを示すために、相互に発行する公開鍵証明書。政府認証基盤では、ブリッジ認証局と政府共用認証局・商業登記認証局・民間認証局それぞれの間で相互認証証明書が発行される。

【タ行】

耐タンパ鍵装置

不正アクセスに備えるための機能(耐タンパ機能)を保有した秘密鍵の管理装置。秘密鍵を管理する特殊なハードウェアであるHSM(Hardware Security Module)を利用する。耐タンパ機能とは、不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正顯示機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。

【ナ行】

認証実施規程(Certification Practice Statement、CPS)

認証局の信頼性・安全性を一般に説明するために、認証局の運用、認証書発行ポリシー、鍵の生成・管理などのキーマネジメント、責任補償に関して、一連の規定を盛り込んだ文書。認証ポリシーが何を運用方針にするのかを決めるのに対して、認証実施規程は運用方針をどのように適用させるのかの手順を示す。

認証パス

自己の認証局から相手の証明書を発行した認証局までをたどる証明書の検証の道筋。

認証ポリシー(Certificate Policy、CP)

認証局が証明書を発行する時の運用方針を記述する文書。

【ハ行】

秘密鍵

公開鍵暗号方式において用いられる公開されていない鍵のこと。秘密鍵が厳重に管理されているという前提で暗号システムの安全性・信頼性が確保される。

ファイアウォール

インターネットなどのネットワークから組織内部のネットワークを保護するためのシステム。通常内部のネットワークから外部へはアクセスできるが、外部から内部のネットワークにアクセスできないような1方向のアクセス設定がとられている。

プロトコル

コンピュータ同士でデータのやり取りをするときの規定全般をさす用語。データ通信に関わるあらゆる手順は、プロトコルによって定義されている。

プロファイル

証明書や失効情報などに含まれるデータの内容を定義したもの。RFC2459により証明書や失効情報についてのプロファイルについて定義されている。

【ラ行】

リフェラル連携

LDAPv3で実現できるディレクトリの機能。ディレクトリ上に実体のない認証情報に対して参照依頼があった場合に、他のリポジトリへ参照するための情報を提供する。

リポジトリ

階層の構造をもったディレクトリ構造の証明書や失効情報を格納するデータベースを指す。ディレクトリともいう。

リンク証明書

認証局(CA)の鍵ペアを更新する場合に発行される証明書であり、旧CA鍵ペアと新CA鍵ペアの関係を保証したもの。

ルート認証局(Root CA)

階層型の認証構造において、最上位に位置する認証局のこと。配下の認証局の公開鍵証明書の発行、失効を管理する。各証明書の信頼のアンカーとなる。

ログファイル

コンピュータ上で行った処理、操作を記録したファイルのこと。履歴ファイルとも、単にログともいう。