

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
平成 19 年 7 月 6 日 改定
平成 20 年 9 月 30 日 改定
行政情報システム関係課長連絡会議了承

「申請・届出等手続の電子化推進のための基本的枠組み」（平成12年3月31日行政情報システム各省庁連絡会議了承）、「霞が関WAN及び政府認証基盤（共通システム）の最適化計画」（平成17年3月31日 各府省情報化統括責任者連絡会議決定。平成19年8月24日改定）に基づく行政機関等側の認証システム（以下「政府認証基盤」という。）の基本的な仕様は、以下のとおりとする。

第1 基本方針

- 1 政府共用認証局が発行する証明書等をブリッジ認証局から申請者に一元的に提供するとともに、各府省において必要となる証明書の有効性検証のための機能をブリッジ認証局において実現することにより、申請者の利便性の向上、政府認証基盤全体の効率的な構築を図る。
- 2 不正アクセス、災害への適切なセキュリティ対策を講ずるとともに、相互認証の基準により政府認証基盤としての一定のセキュリティレベルを維持しつつ、安全性・信頼性を確保する。
- 3 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するものとし、汎用性・拡張性のあるシステムとする。

第2 基本仕様

政府認証基盤を構成するブリッジ認証局及び政府共用認証局の基本仕様は、次のとおりとする。

1 ブリッジ認証局

(1) 構築単位・構造

ブリッジ認証局は、1認証局のみを構築することとし、下位の認証局を設置しない一階層の構造とする。

(2) システム構成

ブリッジ認証局は、次のシステムにより構成する。

- ア ブリッジ認証システム
- イ ブリッジ認証情報格納システム（ブリッジ認証局リポジトリ）
- ウ 統合認証情報公開システム（統合リポジトリ）
- エ 証明書検証システム

(3) 機能

ブリッジ認証局の各システムが保有する機能は、それぞれ次のとおりとする。

ア ブリッジ認証システム

ブリッジ認証システムは、ブリッジ認証局の鍵の生成・管理、証明書の発行等を行うため、次の機能を保有する。

(ア) 鍵管理機能

公開鍵・秘密鍵ペアの生成、鍵の廃棄、署名、鍵のバックアップを行う。秘密鍵は、NIST（National Institute of Standards and Technology：米国標準技術研究所）の FIPS（Federal Information Processing Standards）140-1 レベル 3 又は FIPS140-2 レベル 3 相当以上の耐タンパ鍵装置 HSM（Hardware Security Module）で生成・管理する。

(イ) 証明書項目管理機能

相互認証証明書、自己署名証明書、リンク証明書、操作員等証明書及び証明書の失効リストのプロファイルを登録・更新・参照する。

(ウ) 証明書発行機能

① 証明書のフォーマットは、次のとおりとする。

- ・ ITU-T（International Telecommunications Union - Telecommunications Standardization Sector：国際電気通信連合－電気通信標準化部門）の X.509 v3 とする。
- ・ 証明書の拡張領域のうち、独自拡張領域は使用しない。
- ・ 証明書の日本語の文字コードは、UTF-8（8-bit UCS Transformation Format）String を使用することとし、UCS（Universal multiple-octet coded Character Set）（ISO/IEC10646-1, JIS X 0221）が規定する以外の文字及び外字は使用しない。

② 相互認証証明書、自己署名証明書、リンク証明書及び操作員等証明書の発行・失効要求を生成する。また、当該要求の受付を行い、これら証明書を発行・出力する。

③ 相互認証証明書の交換はオフラインで実施し、当該証明書の要求フォーマットは PKCS (Public Key Cryptography Standards) #10 とする。

④ 相互認証証明書は、複数の署名アルゴリズムで発行することを可能とする。

(I) 証明書失効機能

発行した証明書を失効させ、証明書失効リストの発行を行う。証明書失効リストのフォーマットは ITU-T の X.509 v2 とする。

(オ) 監査ログ機能

証明書の発行、証明書プロファイルの変更等監査対象となる事象のログを採取する。

(カ) 履歴管理・バックアップ機能

証明書の発行・失効の履歴管理、システムの復旧に必要なデータのバックアップを行う。

イ ブリッジ認証情報格納システム (ブリッジ認証局リポジトリ)

ブリッジ認証情報格納システムにおいては、ブリッジ認証システムが発行した証明書等を格納するため、次の機能を保有する。

なお、ブリッジ認証情報格納システムへのアクセスプロトコルは、LDAP (Lightweight Directory Access Protocol) v3 とする。

(ア) 認証情報格納機能

相互認証証明書、自己署名証明書、リンク証明書、操作員等証明書及び証明書の失効情報の格納を行う。

(イ) ディレクトリ参照機能

格納された証明書及び失効情報を参照する。

(ウ) ディレクトリ更新機能

格納された証明書及び失効情報を更新する。

(エ) ログ出力機能

ブリッジ認証情報格納システムに対する処理要求の内容及び処理の結果をログファイルとして出力する。

(オ) バックアップ機能

証明書、失効情報等を定期的にバックアップする。

ウ 統合認証情報公開システム (統合リポジトリ)

統合認証情報公開システムにおいては、申請者の利便性の向上及び政府共用認証局の負担軽減の観点から、各種認証情報を申請・届出等業務アプリケーション等に一元的に提供するため、次の機能を保有す

る。

なお、統合認証情報公開システムへのアクセスプロトコルは、LDAP v3 とする。

(7) 認証情報格納機能

次の認証情報の格納を行う。

- ・ ブリッジ認証システムが発行した相互認証証明書、自己署名証明書、リンク証明書及び証明書の失効情報の複製
- ・ 政府共用認証システムが発行した相互認証証明書、自己署名証明書、リンク証明書及び証明書の失効情報の複製
- ・ ブリッジ認証局と相互認証を行っている民間認証局、国・地方公共団体等が運営する認証局（政府共用認証局を除く。）の証明書等の所在情報

(4) 認証情報公開機能

格納された認証情報をインターネットにより公開し、申請・届出等業務アプリケーション等に認証情報を提供する。

なお、ブリッジ認証局と相互認証を行っている民間認証局、国・地方公共団体等が運営する認証局（政府共用認証局を除く。）の証明書等については、その所在情報を公開し、参照（リフェラル）連携により提供する。

(ウ) ディレクトリ参照機能

格納された証明書及び失効情報を参照する。

(エ) ディレクトリ更新機能

格納された証明書及び失効情報を更新する。

(オ) ログ出力機能

統合認証情報公開システムに対する処理要求の内容及び処理の結果をログファイルとして出力する。

(カ) バックアップ機能

証明書、失効情報等を定期的にバックアップする。

エ 証明書検証システム

証明書検証システムは、各府省において必要となる証明書の有効性の検証に資するため、次の機能を保有する。

なお、各府省の申請・届出等業務アプリケーションと証明書検証システム間の通信プロトコルは、OCSP（Online Certificate Status Protocol）に拡張要素を加えたものとする。

(7) 証明書取得機能

認証パスの構築に必要な証明書を、統合認証情報公開システム及び民間認証局、国・地方公共団体等が運営する認証局（政府共用認証局を除く。）から LDAP v3 プロトコルを使用して取得する。

(イ) 証明書失効リスト取得機能

認証パスの構築に必要な証明書の失効リストを、統合認証情報公開システム及び民間認証局、国・地方公共団体等が運営する認証局（政府共用認証局を除く。）から LDAP v3 プロトコルを使用して取得する。

(ウ) OCSP クライアント機能

証明書の失効情報を OCSP で提供している民間認証局、国・地方公共団体等が運営する認証局（政府共用認証局を除く。）に対し、証明書の検証要求を行う。

(エ) 認証パス構築機能

申請・届出等業務アプリケーションからの要求に応じた認証パスの構築を行う。

(オ) 署名検証機能

証明書に付された署名の検証を行い、署名検証結果を生成する。

(カ) 認証パス有効性検証機能

構築された認証パスの有効性を、取得した証明書失効リスト、OCSP 応答情報を利用して検証する。

(4) セキュリティ対策

ブリッジ認証局においては、次のとおり、物理的、技術的及び人的面からのセキュリティ対策を適切に講ずる。

ア 各システムを設置するための施設設備には、「情報システム安全対策基準」（平成9年9月24日通商産業省告示第536号）等に準拠して、必要な安全対策を講ずる。

イ 各システムの設置に当たっては、セキュリティに配慮し、各システムの機能に応じて室を区画する。特にブリッジ認証システムを設置する区画については、専用の室として整備する。

ウ 各室においては、設置されているシステムの機能に応じ、不正侵入防止のための入退室管理・室内監視設備等を備える。

エ 重要機器等の二重化等によりシステムの冗長性を確保するとともに、操作員等のアクセス権限の設定、ファイアウォールの設置等により不正アクセスの防止を図る。

オ 署名アルゴリズムの鍵長の変更、異なる署名アルゴリズムへの変更

が円滑に行えるシステムとする。

- カ 運営に係る業務を行うに当たっては、責任と権限を明確にして業務遂行の承認・決定等を行う。特に秘密鍵の生成・管理、証明書発行・管理については、複数の人員による相互牽制体制の下で業務を遂行する。
- キ 運営を外部に委託するに当たっては、委託先との秘密保持に関する取り決めを行う。
- ク 上記のほか、「政府機関の情報セキュリティ対策のための統一基準」（２００５年１２月１３日情報セキュリティ政策会議決定）を踏まえ総務省が策定した情報セキュリティポリシーに基づき、必要な措置を講ずる。

(5) 相互認証

ブリッジ認証局が相互認証を行うに当たっての方針及び相互認証の基準は、次のとおりとする。

ア ブリッジ認証局と政府共用認証局

ブリッジ認証局は、政府共用認証局のうち、処分権者の官職を認証するルート認証局とのみ相互認証を行う。

イ ブリッジ認証局と地方公共団体における組織認証基盤のブリッジ認証局

ブリッジ認証局は、地方公共団体における組織認証基盤のブリッジ認証局と相互認証を行う。

ウ ブリッジ認証局と商業登記認証局

ブリッジ認証局は、商業登記制度に基礎を置き、会社・法人の代表者等を認証する認証局と相互認証を行う。

エ ブリッジ認証局と地方公共団体による公的個人認証サービスの公的個人認証サービスブリッジ認証局

ブリッジ認証局は、地方公共団体による公的個人認証サービスの公的個人認証サービスブリッジ認証局と相互認証を行う。

オ ブリッジ認証局と民間認証局

ブリッジ認証局は、「電子署名及び認証業務に関する法律」（平成１２年法律第１０２号）に基づく認定を受け、かつブリッジ認証局との相互認証のために必要な要件を満たした民間認証局と相互認証（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業務の範囲に限る。）を行う。

カ ブリッジ認証局とその他の認証局

その他の認証局との相互認証については、相互認証のために要件等を含め必要に応じて検討する。

(6) 諸規程

ブリッジ認証局の運営に必要な次の諸規程を整備する。

なお、認証ポリシー及び認証実施規程については、IETF (Internet Engineering Task Force) の RFC (Request For Comments) 2527 又は 3647 に準拠して作成する。

ア 認証ポリシー (Certificate Policy)

イ 認証実施規程 (Certification Practice Statement)

ウ 相互認証基準

エ 情報セキュリティの実施手順

オ その他運営に必要なもの

(7) その他

ブリッジ認証局の施設整備に当たっては、政府共用認証局の運営に必要な機器等を収容することが可能なスペースを確保する。

2 政府共用認証局

(1) 構築単位・構造

ア 政府共用認証局は、処分権者の官職を認証するシステムとして 1 認証局 (ルート認証局に下位の認証局を設置する構造を含む。) を構築し、府省等が運営するサーバ、府省等が配布するソフトウェアを認証するシステムとして、1 認証局 (ルート認証局に下位の認証局を設置する構造を含む。) を構築する。

イ ルート認証局に下位の認証局を設置する場合には、ツリー体系による階層構造とし、ルート認証局に対する認証経路が一意に定まる構造とする。

ウ 政府共用認証局は、各府省等の登録業務に基づき証明書の発行指示を受け入れる機能を有する構造とする。

(2) システム構成

政府共用認証局は、次のシステムにより構成する。

ア 政府共用認証システム

イ 政府共用認証情報格納システム (政府共用認証局リポジトリ)

(3) 機能

政府共用認証局の各システムが保有する機能は、それぞれ次のとおりとする。

ア 政府共用認証システム

政府共用認証システムにおいては、政府共用認証局の鍵の生成・管理、証明書発行等を行うため、次の機能を保有する。

(7) 鍵管理機能

公開鍵・秘密鍵ペアの生成、鍵廃棄、署名、鍵のバックアップを行う。秘密鍵は、NIST の FIPS 140-1 レベル 3 又は FIPS140-2 レベル 3 相当以上の耐タンパ鍵装置 HSM で生成・管理する。

(4) 証明書項目管理機能

官職証明書、利用者証明書、サーバ証明書、コード署名証明書、相互認証証明書、自己署名証明書、リンク証明書、操作員等証明書及び証明書の失効リストのプロファイルを登録・更新・参照する。

(ウ) 証明書発行機能

① 証明書のフォーマットは、次のとおりとする。

- ・ ITU-T の X.509 v3 とする。
- ・ 証明書の拡張領域のうち、独自拡張領域は使用しない。
- ・ 証明書の日本語の文字コードは、UTF-8 String を使用することとし、UCS (ISO/IEC10646-1, JIS X 0221) が規定する以外の文字及び外字は使用しない。

② 官職証明書、利用者証明書、サーバ証明書、コード署名証明書、相互認証証明書、自己署名証明書、リンク証明書及び操作員等証明書の発行・失効要求を生成する。また、当該要求の受付を行い、これら証明書を発行・出力する。

③ 相互認証証明書の交換はオフラインで実施し、当該証明書の要求フォーマットは PKCS#10 とする。

④ 相互認証証明書は、複数の署名アルゴリズムで発行することを可能とする。

(イ) 証明書失効機能

発行した証明書を失効させ、証明書失効リストの発行を行う。証明書失効リストのフォーマットは ITU-T の X.509 v2 とする。

(オ) 監査ログ機能

証明書の発行、証明書プロファイルの変更等監査対象となる事象のログを採取する。

(カ) 履歴管理・バックアップ機能

証明書の発行・失効の履歴管理、システムの復旧に必要なデータのバックアップを行う。

イ 政府共用認証情報格納システム(政府共用認証局リポジトリ)

政府共用認証情報格納システムにおいては、政府共用認証システムが発行した証明書等を格納するため、次の機能を保有する。

なお、政府共用認証情報格納システムへのアクセスプロトコルは、LDAP v3 とする。

(ア) 認証情報格納機能

相互認証証明書、自己署名証明書、リンク証明書及び証明書の失効情報の格納を行う。

(イ) ディレクトリ参照機能

格納された証明書及び失効情報を参照する。

(ロ) ディレクトリ更新機能

格納された証明書及び失効情報を更新する。

(ハ) ログ出力機能

政府共用認証情報格納システムに対する処理要求の内容及び処理の結果をログファイルとして出力する。

(ニ) バックアップ機能

証明書、失効情報等を定期的にバックアップする。

(ホ) 統合認証情報公開システムとの連携機能

政府共用認証情報格納システムに格納している相互認証証明書、自己署名証明書、リンク証明書及び証明書の失効情報を複製し、ブリッジ認証局の統合認証情報公開システムに提供する。

(4) セキュリティ対策

ブリッジ認証局(第2-1-(4))に準じてセキュリティ対策を講ずる。

(5) 相互認証

政府共用認証局のうち、処分権者の官職を認証する認証局はブリッジ認証局を介して民間認証局等と相互認証を行うものとし、民間認証局等との間で直接の相互認証は行わない。また、府省等のサーバ、ソフトウェアを認証する認証局は相互認証を行わない。

(6) 諸規程

ブリッジ認証局(第2-1-(6))に準じて諸規程を整備する。

第3 その他

1 基本的な仕様の見直し

この基本的な仕様については、情報通信技術の動向等を踏まえ、必要に

応じて見直すものとする。

2 詳細仕様

- (1) 基本的な仕様を踏まえた詳細な仕様については、行政情報システム関係課長連絡会議等において取りまとめる。
- (2) 詳細な仕様については、政府認証基盤のセキュリティ上の問題を勘案しつつ、可能な範囲で公開するものとする。