

政府認証基盤(GPKI)

行政機関等認証局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

平成15年6月6日改定

平成17年9月1日改定

平成19年3月30日改定

平成19年7月6日改定

平成20年9月30日改定

共通システム専門部会了承

＜構成について＞

- 1 本ガイドラインは、「CP」及び「CPS」をそれぞれ独立したものとせず、「CP」及び「CPS」を一体化した行政機関等認証局CP/CPSを作成するためのものです。
- 2 記述構成は、IETF PKIX (Internet Engineering Task Force Public Key Infrastructure(X.509)) による RFC 2527「Certificate Policy and Certification Practices Statement Framework」に基づいています。
- 3 RFC 2527の主項目(項目階層第2レベルの項目:例「1. 1」)及びサブコンポーネント(項目階層第3レベルの項目:例「1. 3. 1」)まで項目立てしています。

＜行政機関等認証局CP/CPS作成上の留意点＞

- 1 行政機関等認証局の設備、システム、運用等に依存する内容については、各行政機関等の実態に応じて定める必要があります。
- 2 本ガイドラインにおける主項目は必須としますが、サブコンポーネントについては、記述すべき内容を満たしていれば項目立てを変更してもよいこととします。
- 3 行政機関等認証局CP/CPSには、決定年月日及び決定組織を明示するものとします。
- 4 行政機関等認証局CP/CPSにおいて定める内容は「記述内容」欄の記述事項であり、「区分」欄及び「備考」欄は記述対象事項ではありません。

＜「記述内容」欄及び「備考」欄における記号の意味＞

- []: 行政機関等の実態に応じて記述する必要のある箇所
- ※: 記述すべき内容の概要を説明するコメント

＜「区分」欄における記号の意味＞

- A: 行政機関等認証局CP/CPSに記述すべき内容が記載されている項目
- B: 行政機関等の実態に応じて定めるべき内容がある場合に記述する項目

＜RFC3647対応＞

- 1 RFC3647に準拠して記述する場合、本ガイドラインの内容が含まれている必要があります。

記述内容		区分	備考
1. はじめに	本CP/CPSは、国民等と行政機関等[等]との間の申請・届出等手続の電子化を実現するため、総務省が運営するブリッジ認証局(以下「BCA」という。)と相互認証を行い官職の証明書等を発行する行政機関等認証局(以下「行政機関等CA」という。)の認証業務に関する運営方針を定める。 なお、本CP/CPSの構成は、IETF PKIXによる RFC 2527「Certificate Policy and Certification Practices Statement Framework」に準拠している。	A	※本CP/CPSが行政機関等CAのCP/CPSであることを記述す
1. 1 概要	行政機関等CAは、官職に対して[官職]証明書を発行し、BCAと相互認証証明書を取り交わす。 行政機関等CAは、CP(証明書ポリシー)及びCPS(認証実施規程)をそれぞれ独立したものとせず、本CP/CPSを行政機関等CAの認証業務に関する運営方針として位置付ける。	A	※行政機関等CAの認証業務の概要及び本CP/CPSの位置付けを記述する。
1. 2 識別	行政機関等CAの証明書ポリシーの識別子は、次のとおりとする。 行政機関等CA相互認証証明書ポリシー: [x. xx. xxx. xxxxxx. x. x. x. x. x] 行政機関等CA相互認証テスト用証明書ポリシー: [x. xx. xxx. xxxxxx. x. x. x. x. x] [官職]証明書ポリシー: [x. xx. xxx. xxxxxx. x. x. x. x. x]	A	※行政機関等CAの証明書ポリシーを示すオブジェクト識別子(OID)を記述する。 ※サーバ証明書等他の証明書を発行する場合は、その証明書ポリシーの識別子を記述する。
1. 3 運営体制と証明書の適用範囲	1. 3. 1 CAの組織 (1) 意思決定組織 行政機関等CAの運営に関する意思決定は、[行政機関等CA運営委員会]が行う。 [行政機関等CA運営委員会]の機能は、次のとおりとする。 ・ 行政機関等CAのCP/CPSに関する決定 ・ 相互認証に関する決定 ・ CA秘密鍵危殆化時の対応に関する決定 ・ 災害発生等による緊急時の対応に関する決定 ・ その他行政機関等CAの運営に関する重要事項の決定 (2) [行政機関等CA〇〇組織] [BCAへの相互認証申請、行政機関等における[官職]証明書発行申請の受付及び審査並びに相互認証証明書、[官職]証明書等の発行、更新、失効等の運営業務は、行政機関等CA責任者、IA鍵管理者、受付担当者及び審査担当者が行う。 また、システムオペレーション、システムの維持管理等の運用業務は、IA操作員、RA操作員、ディレクトリ操作員及び監査ログ検査者が行う。それぞれの業務については、「5. 2 手続面の管理」において定める。]	A	※行政機関等CAの運営体制を示し、その業務を記述する。
1. 3. 2 証明書の適用範囲	BCAに対して相互認証証明書を発行する。相互認証証明書の有効期間は、証明書を有効とする日から起算して5年[以下]とする。 [官職(独立行政法人、公社、特殊法人、認可法人及び指定法人のものを含む。以下同じ。)]に対して[官職]証明書を発行する。[官職]証明書の有効期間は、証明書を有効とする日から起算して3年[以下]とする。	A	※行政機関等CAの発行する証明書の発行対象及び適用範囲を記述する。なお、CAが階層構造を取っている場合は、CAごとに記述する。 ※サーバ証明書等他の証明書を発行する場合は、当該証明書を行政機関等CAが発行する証明書の適用範囲として記述する。
1. 4 CP/CPSに関する担当組織	1. 4. 1 管理担当部署 本CP/CPSの変更、更新等に関する事務は、[〇〇局〇〇課]が行う。	A	※本CP/CPSに関する連絡先について記述する。
1. 4. 2 照会窓口	本CP/CPSに関する照会は、[〇〇局〇〇課]を窓口とする。	A	

記述内容		区分	備考
2. 一般規定			
2. 1 義務			※CA、RA等において、それぞれが負う義務について記述する。
2. 1. 1	CA業務に関する義務 行政機関等CAは、CA業務に関して次の義務を負う。 ・BCAへの相互認証申請に際して、正確な情報を提示する。 ・本CP/CPSに基づき、自己署名証明書、リンク証明書、相互認証証明書、[官職]証明書等を発行する。 ・相互認証証明書の取り交わしに関しては、BCAの定めた手続に従う。 ・証明書の失効処理を行い、有効期間48時間の失効リスト(以下「CRL/ARL」という。)を24時間ごとに発行する。 ・CA秘密鍵を安全に管理する。 ・CA秘密鍵が危殆化した場合は、速やかにBCA運営組織に報告する。 ・証明書の発行、更新、失効等に関する監査ログ及びアーカイブデータを必要な期間保管する。 ・システムの稼働監視を行う。	A	※サーバ証明書等他の証明書を発行する場合は、関連してCAが負う義務について記述する。
2. 1. 2	RA業務に関する義務 行政機関等CAは、RA業務に関して次の義務を負う。 ・行政機関等CAは、BCAからの相互認証証明書発行要求に含まれる公開鍵が確実にBCAの公開鍵であり、かつBCAがこの公開鍵に対応する秘密鍵を保有していることを確認する。 ・[官職]証明書の発行等の申請手続が適切に行われていることを確認する。	A	
2. 1. 3	証明書利用者の義務 [官職]証明書の利用者は、次の義務を負う。 ・[官職]証明書は、法令に基づき本CP/CPSに従って利用する。 ・[官職]証明書及び官職の秘密鍵を安全に管理する。 ・[官職]証明書の管理は、[文書管理規程又は公印管理規程等]に基づいて行う。 ・秘密鍵が危殆化した場合は、速やかに[行政機関等CA〇〇組織]に報告する。	A	※他の証明書利用者について、負う義務があれば記述する。
2. 1. 4	証明書検証者の義務 [官職]証明書の証明書検証者は、次の義務を負う。 ・証明書検証の際に、証明書の有効性及び認証パスの有効性について検証する。	A	
2. 1. 5	リポジトリに関する義務 行政機関等CAに関する情報のうち公表する情報は、BCAによって運用される統合リポジトリに複製する。	A	
2. 2	CAの責任 行政機関等CAは、自己署名証明書、リンク証明書、相互認証証明書、[官職]証明書等の発行、更新、失効、保管及び公表に当たっては、BCA、証明書利用者及び証明書検証者に対し、本CP/CPSに基づく認証業務を適切に行う。	A	※行政機関等CAが認証業務を行うに当たって負う責任について記述する。 ※サーバ証明書等他の証明書を発行する場合は、負う責任について記述する。
2. 3	財務上の責任 規定しない。	B	※行政機関等CAが負う財務上の責任について記述する。
2. 4	解釈及び執行		
2. 4. 1	準拠法 本CP/CPSに基づく認証業務から生ずる紛争については、日本国の法令を適用する。	A	※本CP/CPSが準拠する法律を記述する。
2. 4. 2	分割、存続、合併及び通知 規定しない。	B	※行政機関等CAの分割、合併などにおける本CP/CPSの有効性について記述する。
2. 4. 3	紛争解決の手続 規定しない。	B	※紛争解決の手続について記述する。
2. 5	料金 規定しない。	B	※証明書の発行、失効情報へのアクセス等に関する料金を記述する。

記述内容	区分	備考
<p>2. 6 公表とリポジットリ</p> <p>2. 6. 1 CAに関する情報の公表 行政機関等CAに関する情報は、BCAの統合リポジットリ及びWeb上で公表する。 (1)BCAの統合リポジットリ上での公表 行政機関等CAは、行政機関等CAリポジットリに保有する次の情報をBCAの統合リポジットリに複製し、統合リポジットリ上で公表する。 ・ 行政機関等CAが発行した自己署名証明書、リンク証明書、相互認証証明書[、官職証明書]等 ・ 行政機関等CAが発行した自己署名証明書、リンク証明書、相互認証証明書、[官職]証明書等のCRL/ARL (2)Web上での公表 行政機関等CAは、次の情報をWeb上で公表する。 ・ 行政機関等CAと相互認証したCAの名称及び相互認証を取消したCAの名称 [・ 行政機関等CAが認証した官職の名称及び認証を取消した官職の名称] ・ CA秘密鍵危殆化に関する情報 ・ 本CP/CPS</p> <p>2. 6. 2 公表の頻度 公表する情報の更新頻度は次のとおりとする。 ・ 行政機関等CAが発行した自己署名証明書、リンク証明書、相互認証証明書[、官職証明書]等は、発行及び更新の都度 ・ 行政機関等CAが発行した自己署名証明書、リンク証明書、相互認証証明書、[官職]証明書等のCRL/ARLは、発行及び更新の都度 ・ 行政機関等CAと相互認証したCAの名称及び相互認証を取消したCAの名称は、[行政機関等CA運営委員会]による決定の都度 [・ 行政機関等CAが認証した官職の名称及び認証を取消した官職の名称は、行政機関等CA運営委員会による決定の都度] ・ 本CP/CPSの変更の都度</p> <p>2. 6. 3 アクセス制御 行政機関等CAリポジットリから複製したBCAの統合リポジットリ上で公表する情報及びWeb上で公表する情報は、インターネットを通じて提供する。 公表情報を提供するに当たっては、特段のアクセス制御は行わない。</p> <p>2. 6. 4 リポジットリ 行政機関等CAリポジットリに保有する情報のうち、「2. 6. 1 CAに関する情報の公表(1)BCAの統合リポジットリ上での公表」において定める情報をBCAの統合リポジットリに複製し公表する。</p>	<p>A</p> <p>A</p> <p>A</p> <p>A</p>	<p>※統合リポジットリ又はWeb上に公表する情報、公表の頻度、公表する情報へのアクセス制御の有無等を記述する。</p> <p>※サーバ証明書等他の証明書を統合リポジットリ上で公表する場合は、当該証明書を記述する。</p> <p>※行政機関等CAに対する監査頻度、監査主体、監査テーマ、監査結果の扱い等について記述する。</p>
<p>2. 7 準拠性監査</p> <p>2. 7. 1 監査頻度 [行政機関等CA〇〇組織]は監査人による監査を年1回定期的に実施する。また、[行政機関等CA〇〇組織]は、必要に応じて定期監査以外に監査を実施する。</p> <p>2. 7. 2 監査人の身元・資格 行政機関等CAの監査は、監査業務及び認証業務に精通した者が行う。</p> <p>2. 7. 3 監査人と被監査部門の関係 行政機関等CAの監査を実施する監査人は、行政機関等CAと利害関係を有しない者を選定する。</p> <p>2. 7. 4 監査テーマ 認証業務が本CP/CPS及び運用マニュアルに準拠して実施されていること[、並びに外部からの不正及び内部の不正行為に対する措置が適切に講じられていること]を中心に監査を実施する。</p> <p>2. 7. 5 監査指摘事項への対応 行政機関等CAは、重要又は緊急を要する監査指摘事項について、[行政機関等CA運営委員会]の決定に基づき速やかに対応する。CA秘密鍵の危殆化に関する指摘があった場合は緊急事態と位置付け、緊急時対応の手続をとる。重要又は緊急を要する監査指摘事項が改善されるまでの間、行政機関等CAの運用を停止するか否かは[行政機関等CA運営委員会]が決定する。また、[行政機関等CA運営委員会]は、監査指摘事項に対して行政機関等CAが対策を実施したことを確認する。</p> <p>2. 7. 6 監査結果 行政機関等CAの監査結果は、監査人から[行政機関等CA〇〇組織]に対して監査報告書として提出される。[行政機関等CA〇〇組織]は、[行政機関等CA運営委員会]及びBCA運営組織に監査結果を報告する。監査報告書は、5年間保管する。</p>	<p>A</p> <p>A</p> <p>A</p> <p>A</p> <p>A</p> <p>A</p>	

記述内容		区分	備考
2.8	機密保持		※機密扱いとする情報、機密扱いとしない情報、情報開示に関する規定等を記述する。
2.8.1	機密扱いとする情報 行政機関等CAは、漏えいすることによって行政機関等CA及びBCAの認証業務の信頼性が損なわれる恐れのある情報を機密扱いとする。機密扱いとする情報は、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に保管管理する。	A	
2.8.2	機密扱いとしない情報 行政機関等CAが保有する情報のうち、証明書、失効情報、本CP/CPS等、公表する情報として明示的に示すものは機密扱いとしない。	A	
2.8.3	証明書失効情報の公表 行政機関等CAは、自己署名証明書、リンク証明書、相互認証証明書、[官職]証明書等の失効情報を公表する。	A	※サーバ証明書等他の証明書の失効情報を公表する場合は、その証明書失効情報の公表について記述する。
2.8.4	法執行機関への情報開示 規定しない。	B	
2.8.5	民事手続上の情報開示 規定しない。	B	
2.8.6	証明書利用者の要求に基づく情報開示 規定しない。	B	
2.8.7	その他の理由に基づく情報開示 規定しない。	B	
2.9	知的財産権 規定しない。	B	※生成する鍵ペア、発行する証明書、証明書の中で使用する名前等の知的財産権に関する規定及びCP/CPSの著作権に関する規定を記述する。
3.	識別と認証		
3.1	初期登録		※証明書で使用される名前に関する規則を記述する。また、証明書発行対象をどのようにして識別・認証するかを記述する。
3.1.1	名前の型 行政機関等CAが発行する証明書の発行者名及び主体者名は、X.500識別名(DN:Distinguished Name)の形式に従って設定する。	A	
3.1.2	名前の意味に関する要件 発行する証明書において使用する名前は、府省、認証局、官職等の名称とする。	A	
3.1.3	名前形式を解釈するための規則 名前の形式を解釈するための規則は、BCAの定める規則に従う。	A	
3.1.4	名前の一意性 行政機関等CAが発行する証明書の主体者名は、一意に割り当てる。	A	
3.1.5	名前に関する紛争の解決手順 規定しない。	B	
3.1.6	商標の認識・認証・役割 規定しない。	B	

	記述内容	区分	備考
	<p>3. 1. 7 秘密鍵の所有を証明するための方法</p> <p>行政機関等CAは、相互認証手続において、BCAから提出された証明書発行要求の署名の検証を行い、含まれているCA公開鍵に対応するCA秘密鍵で署名されていることを確認する。また、証明書発行要求のフィンガープリントを確認し、CA公開鍵の所有者を特定する。 [官職証明書発行手続においては、行政機関等CA側で秘密鍵と公開鍵が対応する鍵ペアを生成する。]</p>	A	<p>※証明書発行対象の公開鍵がその秘密鍵と対をなすものであることを確認する方法を記述する。</p> <p>※サーバ証明書等他の証明書発行対象がある場合は、証明書発行対象の公開鍵がその秘密鍵と対をなすものであることを確認する方法を記述する。</p>
	<p>3. 1. 8 組織の認証</p> <p>行政機関等CAは、相互認証手続において、所定の手続に基づき、相互認証先のCAを運営する者の真偽を確認する。</p>	A	<p>※証明書発行対象が組織の場合は、その識別・認証をどのように行うかを記述する。</p>
	<p>3. 1. 9 個人の認証</p> <p>行政機関等CAは、所定の手続に基づき、証明書の発行申請を行う者の真偽を確認する。</p>	A	<p>※証明書発行対象が個人の場合は、その識別・認証をどのように行うかを記述する。</p>
	<p>3. 2 証明書の更新</p> <p>証明書更新時における識別と認証は、「3. 1 初期登録」において定める手続に基づいて行う。</p>	A	<p>※証明書の更新に当たって、証明書発行対象をどのようにして識別・認証するかを記述する。</p>
	<p>3. 3 証明書失効後の再発行</p> <p>証明書失効後の再発行時における識別と認証は、「3. 1 初期登録」において定める手続に基づいて行う。</p>	A	<p>※証明書失効後の再発行に当たって、証明書発行対象をどのようにして識別・認証するかを記述する。</p>
	<p>3. 4 証明書の失効申請</p> <p>証明書の失効時における識別と認証は、「3. 1. 8 組織の認証」及び「3. 1. 9 個人の認証」において定める手続に基づいて行う。</p>	A	<p>※証明書の失効に当たって、証明書失効対象をどのようにして識別・認証するかを記述する。</p>
4. 運用要件			
	<p>4. 1 証明書の発行申請</p> <p>(1) 相互認証証明書 BCAに対する相互認証証明書の発行申請は、BCAの定める手続に基づいて行う。</p>	A	<p>※証明書の発行申請手続について記述する。</p>
	<p>(2) [官職]証明書 [官職証明書の発行申請は、所定の手続に基づいて行う。]</p>	A	<p>※サーバ証明書等他の証明書を発行する場合は、その発行申請手続について記述する。</p>
	<p>4. 2 証明書の発行</p> <p>(1) 相互認証証明書 行政機関等CAは、BCAの定める手続に基づく接続テスト完了後、BCAから提出された証明書発行要求に対し、自CAの署名を付して相互認証証明書を発行する。</p>	A	<p>※証明書の発行手続について記述する。</p>
	<p>(2) [官職]証明書 [行政機関等CAは、行政機関等CA側で生成した公開鍵に、自CAの署名を付して官職証明書を発行する。]</p>	A	<p>※サーバ証明書等他の証明書を発行する場合は、その証明書の発行手続について記述する。</p>

記述内容	区分	備考
<p>4. 3 証明書の受入れ</p> <p>(1) 相互認証証明書 行政機関等CAは、発行した相互認証証明書を、所定の手続に基づき、BCAに渡し受領書を受け取る。この受領確認をもって相互認証証明書の受入れの完了とする。</p> <p>(2) [官職]証明書 [行政機関等CAは、発行した官職証明書を、所定の手続に基づき安全かつ確実な方法で申請者に配付し受領書を受け取る。この受領確認をもって官職証明書の受入れの完了とする。]</p>	A	※証明書の受入れ手続について記述する。
<p>4. 4 証明書の失効と一時停止</p>		※証明書の一時停止と失効について、該当する事由、申請者、処理手順、一時停止及び失効情報の提供方法等を記述する。
<p>4. 4. 1 証明書の失効理由</p> <p>(1) 相互認証証明書 行政機関等CAは、行政機関等CA又はBCAに次の相互認証証明書失効事由が発生した場合、相互認証証明書を失効する。 ・CA秘密鍵の危殆化 ・相互認証基準違反 ・相互認証業務の終了 ・相互認証更新</p> <p>(2) [官職]証明書 [行政機関等CAは、次の[官職]証明書失効事由が発生した場合、[官職]証明書を失効する。 ・[官職]証明書の秘密鍵の紛失、危殆化 ・CA秘密鍵の紛失、危殆化 ・[官職名の変更、廃止]</p>	A	
<p>4. 4. 2 証明書の失効申請者</p> <p>(1) 相互認証証明書 ア BCAから相互認証証明書失効申請を受ける場合 BCAから行政機関等CAに対する失効申請は、BCAの責任者が行う。</p> <p>イ BCAに相互認証証明書失効申請を行う場合 行政機関等CAからBCAに対する失効申請は、行政機関等CAの責任者が行う。</p> <p>(2) [官職]証明書 [官職証明書の失効申請は、官職証明書の管理者が行う。]</p>	A	
<p>4. 4. 3 証明書の失効申請及び失効処理手順</p> <p>(1) 相互認証証明書 ア BCAから相互認証証明書失効申請を受ける場合 「3. 1. 8 組織の認証」において定める手続を行ったうえで、相互認証証明書を失効し、ARLを統合リポジトリに登録する。</p> <p>イ BCAに相互認証証明書失効申請を行う場合 BCAとの相互認証証明書を失効し、ARLを統合リポジトリに登録する。</p> <p>(2) [官職]証明書 [官職証明書の失効申請を受け取った行政機関等CAは、その失効申請が所定の手続に基づいていることを確認したうえで、要求された官職証明書を失効し、CRLをBCAの統合リポジトリに複製する。]</p>	A	
<p>4. 4. 4 失効における猶予期間 行政機関等CAは、失効申請手続の終了後、直ちに失効処理を行う。</p>	A	
<p>4. 4. 5 一時停止 行政機関等CAは、証明書の一時停止を行わない。</p>	A	
<p>4. 4. 6 一時停止申請者 規定しない。</p>	B	

記述内容	区分	備考
4.4.7 一時停止手順 規定しない。	B	
4.4.8 一時停止期間の制限 規定しない。	B	
4.4.9 CRL/ARLの発行周期 有効期間48時間のCRL/ARLを24時間ごとに発行する。ただし、CA秘密鍵の危殆化等が発生した場合は、CRL/ARLを直ちに発行する。	A	
4.4.10 CRL/ARLの確認 証明書検証者は、行政機関等CAの発行するCRL/ARLによって証明書の有効性を確認しなければならない。行政機関等CAは、この確認が行えるようBCAの統合リポジトリ上でCRL/ARLを公表する。	A	
4.4.11 オンライン有効性確認の可用性 統合リポジトリは、BCAが維持管理する。	A	
4.4.12 オンライン有効性確認要件 規定しない。	B	※オンライン有効性確認に関して、証明書検証者に課す要件があれば記述する。
4.4.13 その他利用可能な有効性確認手段 規定しない。	B	※前述以外の方法で証明書の有効性確認手段を有する場合は、その内容を記述する。
4.4.14 その他利用可能な有効性確認手段における確認要件 規定しない。	B	
4.4.15 秘密鍵の危殆化に関する特別な要件 規定しない。	B	
4.5 セキュリティ監査の手順		※監査ログの検査に関して、記録されるログの種類、検査周期、保管期間、保護方法、バックアップ手順、収集システム等を記述する。
	A	監査ログ検査者は、行政機関等CAシステム及び行政機関等CAリポジトリにおける発生事象を記録したログ(以下「監査ログ」という。)を業務実施記録等と照合し、不正操作等異常な事象を確認するセキュリティ監査を行う。
4.5.1 監査ログに記録する情報 行政機関等CAシステム及び行政機関等CAリポジトリにおけるセキュリティに関する重要な事象を対象に、アクセスログ、操作ログ等監査ログを記録する。監査ログには、次の情報を含める。 ・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(操作員名、システム名等)	A	
4.5.2 監査ログの検査周期 監査ログ検査者は、業務実施記録等と監査ログとの照合を[週次]で行う。	A	
4.5.3 監査ログの保管期間 監査ログは、[3年間]保管する。	A	
4.5.4 監査ログの保護 監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。 監査ログのバックアップは、[週次]で外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。 なお、監査ログの閲覧及び削除は監査ログ検査者が行う。	A	

記述内容	区分	備考
4.5.5 監査ログのバックアップ手順 監査ログは[日次]でバックアップし、[週次]で外部記憶媒体に取得する。	A	
4.5.6 監査ログの収集システム 監査ログの収集機能はCAシステムの一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。	A	
4.5.7 監査ログ検査の通知 監査ログの検査は、事象を発生させた者に通知することなく行う。	A	※監査ログ検査時の、事象を発生させた者への通知の有無を記述する。
4.5.8 脆弱性の評価 監査ログを検査することにより、運用面及びシステム面におけるセキュリティ上の脆弱性を評価する。	A	
4.6 アーカイブ 4.6.1 アーカイブデータの種類 アーカイブデータは、次のものとする。 ・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	A	※アーカイブに関して、対象データの種類、保管期間、保護方法、バックアップ手順、タイムスタンプに関する要件等を記述する。 ※その他、アーカイブデータの対象となるものがある場合は記述する。
4.6.2 アーカイブデータの保管期間 アーカイブデータは、[該当する証明書の有効期間満了日から10年間]保管する。	A	
4.6.3 アーカイブデータの保護 アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。アーカイブデータのバックアップは、[月次]で外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。	A	
4.6.4 アーカイブデータのバックアップ手順 アーカイブデータは[日次]でバックアップし、[月次]で外部記憶媒体に取得する。	A	
4.6.5 レコードのタイムスタンプに関する要件 アーカイブデータには、レコード単位でタイムスタンプを付与する。	A	
4.6.6 アーカイブデータの収集システム 規定しない。	B	
4.6.7 アーカイブデータの検証 アーカイブデータが記録された外部記憶媒体の可読性の確認を、[年1回]行う。	A	
4.7 鍵更新 5年ごとにCA鍵ペアの更新を行う。 ただし、公開鍵と秘密鍵の有効期間内に行政機関等CAを廃止する場合は、この限りでない。 CA鍵ペア更新時には、古いCA公開鍵と新しいCA公開鍵の認証パスを構築するリンク証明書を発行し、BCAの統合リポジトリ上で公表する。	A	※行政機関等CAのCA鍵ペアの更新時におけるCA公開鍵の配付手順を記述する。
4.8 危殆化と災害からの復旧		
4.8.1 ハードウェア、ソフトウェア又はデータが破壊された場合の対処 ハードウェア、ソフトウェア又はデータが破壊された場合、バックアップ用のハードウェア、ソフトウェア又はデータにより、速やかに復旧作業を行う。	A	
4.8.2 証明書を失効する場合の要件 発行した証明書の失効処理に当たっては、その失効の取消しは行わない。証明書を失効した証明書利用者に対し、再度証明書を発行する場合は、あらかじめ発行手続を行う。	A	

記述内容	区分	備考
4.8.3 秘密鍵が危殆化した場合の対処 CA秘密鍵が危殆化した場合は、[危機管理計画]に基づいて認証業務を停止し、次の手続を行う。 ・相互認証証明書、[官職]証明書等の失効手続 ・CA秘密鍵の廃棄及び再生成手続 ・相互認証証明書、[官職]証明書等の再発行手続 また、証明書利用者の秘密鍵が危殆化した場合は、「4.4 証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。	A	
4.8.4 災害等発生時の設備の確保 災害等により行政機関等CAの設備が被害を受けた場合は、予備機を確保しバックアップデータを用いて運用を行う。	A	
4.9 認証業務の終了 [行政機関等CA運営委員会]において行政機関等CAの認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の行政機関等CAのバックアップデータ、アーカイブデータ等の保管組織及び開示方法を業務終了90日前までに証明書利用者及び証明書検証者に告知し、所定の業務終了手続を行う。	A	※行政機関等CAの認証業務を終了する場合は、予告期間、手順等を記述する。
5. 物理面、手続面及び人事面のセキュリティ管理		
5.1 物理的管理		
5.1.1 施設の位置と建物構造 行政機関等CAの施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。	A	
5.1.2 物理的アクセス 施設内の各室内において行われる認証業務の重要度に応じ、複数のセキュリティレベルで入退室管理を行う。認証は、操作権限者が識別できるICカード及び生体認証装置により行う。 各室への入退室権限は、「5.2 手続面の管理」において定める各要員の業務に応じて[行政機関等CA責任者]が付与する。 行政機関等CAの施設は、監視員を配置して監視システムにより24時間365日監視を行う。	A	
5.1.3 電源設備と空調設備 行政機関等CAは、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講ずる。商用電源が供給されない事態においては、一定時間内に発電機による電源供給に切り換える。 また、空調設備を設置することにより機器類の動作環境及び要員の作業環境を適切に維持する。	A	
5.1.4 水害対策 行政機関等CAの設備を設置する建物、室には漏水検知器を設置し、天井、床には防水対策を講ずる。	A	
5.1.5 地震対策 行政機関等CAの設備を設置する建物は耐震構造とし、機器・什器の転倒及び落下を防止する対策を講ずる。	A	
5.1.6 火災対策 行政機関等CAの設備を設置する建物は耐火構造、室は防火区画とし、消火設備を備える。	A	
5.1.7 媒体管理 アーカイブデータ、バックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続に基づき適切に搬出入管理を行う。	A	
5.1.8 廃棄物処理 機密扱いとする情報を含む書類・記憶媒体の廃棄については、所定の手続に基づいて適切に廃棄処理を行う。	A	
5.1.9 オフサイトバックアップ 重要なデータ等の媒体を別地保管するに当たっては、移送経路のセキュリティを確保するとともに、媒体の保管のための施設には行政機関等CAの施設と同等のセキュリティ対策を講ずる。	B	※バックアップデータの別地保管を行う場合は記述する。

	記述内容	区分	備考
5. 2 手続面の管理	<p>相互認証証明書、[官職]証明書等の発行、更新、失効等の重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。</p> <p>重要な業務の指示は、[行政機関等CA責任者]が各操作員に対して作業指示書によって指示する。</p> <p>操作員がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別・認証を行う。</p> <p>各要員の業務を次のとおり定める。</p>	A	<p>※認証業務の要員及びその業務を定義し、権限分離を行うことを明確に記述する。業務を追加又は削除する場合も、権限分離の考え方を明示する。</p>
	<p>(1) [行政機関等CA責任者]</p> <p>[行政機関等CA責任者は、行政機関等CAの運営に関する責任者であり、次の業務を行う。]</p> <ul style="list-style-type: none"> 行政機関等CA運営方針の策定 認証業務の統括 CA秘密鍵の危殆化発生時、災害発生時等緊急時における対応の統括 IA操作員、RA操作員等への作業指示及び作業結果の確認 その他行政機関等CAの運営及び運用に関する統括] 	A	
	<p>(2) IA鍵管理者</p> <p>IA鍵管理者は、CA秘密鍵を使用する業務に関する責任者であり、次の業務を行う。なお、操作は複数人のIA鍵管理者が行う。</p> <ul style="list-style-type: none"> HSMの機能を制御する鍵(以下「管理鍵」という。)の保管管理 CA秘密鍵のバックアップ媒体の保管管理 CA秘密鍵生成、自己署名証明書発行時のHSMに対する鍵操作 CA秘密鍵の更新時におけるHSMに対する鍵操作 CA秘密鍵のバックアップ、バックアップからのリストア時のHSMに対する鍵操作およびCA秘密鍵のバックアップ媒体のセット 	A	
	<p>(3) 受付担当者</p> <p>受付担当者は、BCAからの相互認証証明書の発行要求の受付、[官職]証明書等の発行申請の受付、申請者との連絡調整業務及び申請書類等の管理を行う。</p>	A	
	<p>(4) 審査担当者</p> <p>審査担当者は、[官職]証明書等の発行申請の審査業務を行う。</p>	A	
	<p>(5) [IA操作員]</p> <p>[IA操作員は、CA秘密鍵を使用する次の業務を行う。なお、操作は複数人のIA操作員が行う。]</p> <ul style="list-style-type: none"> CA秘密鍵(HSM)の活性化・非活性化 行政機関等CAシステムの起動・停止 行政機関等CAシステムの動作に関する設定変更管理 行政機関等CAシステムのデータベースのバックアップに関する諸設定管理並びにバックアップ、リストア及びアーカイブの操作] 	A	
	<p>(6) [RA操作員]</p> <p>[RA操作員は、行政機関等CAシステムが発行する証明書に関する次の業務を行う。なお、操作は複数人のRA操作員が行う。]</p> <ul style="list-style-type: none"> 証明書ポリシーの設定登録、変更 相互認証証明書、[官職]証明書等の発行、更新及び失効処理 操作員への証明書の発行、更新及び失効処理] 	A	
	<p>(7) [ディレクトリ操作員]</p> <p>[ディレクトリ操作員は、行政機関等CAリポジトリの設定管理に関する業務を行う。]</p>	A	
	<p>(8) 監査ログ検査者</p> <p>監査ログ検査者は、行政機関等CAシステム及び行政機関等CAリポジトリのログに関する次の業務を行う。</p> <ul style="list-style-type: none"> 監査ログの検査 不要な監査ログの削除 	A	<p>※監査ログ検査者は、行政機関等CAシステムの操作権限が付与されていない者とする。</p>
5. 3 人事面の管理	<p>行政機関等CAの要員の適格性の審査、教育、配置転換等については、国家公務員法等人事関係法令に基づいて運用する。また、すべての要員には、行政機関等CAの運営を行うために必要な知識及び技術を習得するための教育訓練を行う。</p>	A	

記述内容	区分	備考
<p>6. 技術的セキュリティ管理</p> <p>6. 1 鍵ペア生成とインストール</p> <p>6. 1. 1 鍵ペア生成</p> <p>(1) CA鍵 CA鍵ペアは、複数人のIA鍵管理者が[FIPS140-1レベル3相当]のHSMを用いて生成する。</p> <p>(2) [官職]証明書鍵 [官職]証明書の鍵ペアは、RA操作員がFIPS140-1レベル3相当のHSMを用いて生成する。]</p>	A	<p>※鍵ペアの生成について、生成する装置の技術水準と生成する要員を記述する。</p> <p>※CA鍵のHSMは、「FIPS140-1レベル3」以上の技術水準を記述する。</p> <p>※官職証明書の鍵ペアの生成について、その生成装置及び要員による安全かつ確実な運用について記述する。</p> <p>※サーバ証明書の鍵ペア等、他の鍵ペアを生成する場合は、その生成装置及び要員による安全かつ確実な運用を記述する。</p>
<p>6. 1. 2 証明書利用者への秘密鍵配付</p> <p>[官職証明書の秘密鍵は、「6. 2. 1 暗号モジュールに関する基準」において定める暗号モジュールに格納し、所定の手続に基づいて配付する。]</p>	A	<p>※生成した官職証明書の秘密鍵を安全に配付することを記述する。</p>
<p>6. 1. 3 公開鍵の受領</p> <p>行政機関等CAは、相互認証証明書の取り交わしにおいて、BCAの公開鍵を安全かつ確実に受取る。</p>	A	<p>※公開鍵の受領方法について記述する。</p> <p>※サーバ証明書に対する公開鍵等、他に行政機関等CAへ公開鍵を送付する場合はその受領方法について記述する。</p>
<p>6. 1. 4 CA公開鍵の配付</p> <p>行政機関等CA内の証明書利用者及び証明書検証者に安全かつ確実な手段で配付する。</p>	A	<p>※行政機関等CAのCA公開鍵を行政機関等CA内証明書利用者及び証明書検証者に提供する方法を記述する。</p>
<p>6. 1. 5 鍵のサイズ</p> <p>(1) CA鍵 RSA2048ビットの鍵を使用する。</p> <p>(2) [官職]証明書鍵 RSA1024ビットの鍵を使用する。</p>	A	<p>※行政機関等CAのCA鍵ペア及び官職証明書の鍵ペアについて、アルゴリズムと鍵長を記述する。</p> <p>※その他の鍵ペアを生成する場合は、そのアルゴリズムと鍵長を記述する。</p>
<p>6. 1. 6 公開鍵のパラメータの生成</p> <p>規定しない。</p>	B	<p>※公開鍵パラメータの生成方法を記述する。</p> <p>※準拠している規格がある場合は記述する。</p>
<p>6. 1. 7 公開鍵パラメータの品質の検査</p> <p>規定しない。</p>	B	<p>※公開鍵パラメータの品質検査方法を記述する。</p> <p>※準拠している規格がある場合は記述する。</p>
<p>6. 1. 8 鍵を生成するハードウェア/ソフトウェア</p> <p>「6. 1. 1 鍵ペア生成」において定める。</p>	A	<p>※鍵ペアを生成するハードウェア/ソフトウェアについて記述する。</p>
<p>6. 1. 9 鍵の利用目的</p> <p>(1) CA鍵 CA秘密鍵は、署名に用いる。</p> <p>(2) [官職]証明書鍵 [官職]証明書の秘密鍵は、署名に用いる。</p>	A	<p>※証明書ポリシー(X.509 v3)のKey Usageに定義する内容について記述する。</p> <p>※他の鍵ペアを生成する場合は、その秘密鍵の利用目的について記述する。</p>

記述内容	区分	備考
<p>6.2 秘密鍵の保護</p> <p>6.2.1 暗号モジュールに関する基準</p> <p>(1)CA鍵 CA秘密鍵は、[FIPS140-1レベル3相当]のHSMにより保護する。</p> <p>(2)[官職]証明書鍵 [官職]証明書の秘密鍵は、FIPS140-1レベル2相当以上の[Cカード]により保護する。</p>	A	<p>※秘密鍵の保護で使用する暗号モジュールの技術水準を記述する。 ※CA鍵のHSMは、「FIPS140-1レベル3」以上の技術水準を記述する。 ※他の鍵ペアを生成する場合は、その秘密鍵の保護に使用する暗号モジュールについて記述する。</p>
<p>6.2.2 秘密鍵の複数人制御</p> <p>CA秘密鍵を使用する操作は、複数人のIA鍵管理者が行う。</p>	A	<p>※行政機関等CAの秘密鍵を使用する操作が複数人によって行われることを記述する。</p>
<p>6.2.3 秘密鍵の預託</p> <p>秘密鍵の預託は行わない。</p>	A	<p>※官職証明書等の秘密鍵の預託有無を記述する。</p>
<p>6.2.4 秘密鍵のバックアップ</p> <p>CA秘密鍵のバックアップは、複数人のIA鍵管理者が行う。 HSMからバックアップしたCA秘密鍵は、[暗号化して複数に分割し、複数人のIA鍵管理者によって]安全に保管する。</p>	A	<p>※行政機関等CAのCA秘密鍵のバックアップ手順及び保管方法について、記述する。</p>
<p>6.2.5 秘密鍵のアーカイブ</p> <p>秘密鍵のアーカイブは行わない。</p>	A	<p>※秘密鍵のアーカイブを行うか否かを記述する。</p>
<p>6.2.6 暗号モジュールへの秘密鍵の格納</p> <p>(1)CA鍵 CA秘密鍵は、複数人のIA鍵管理者が暗号モジュールの中で生成し、格納する。</p> <p>(2)[官職]証明書鍵 [官職]証明書の秘密鍵は、RA操作員が暗号モジュールの中で生成し、格納する。]</p>	A	<p>※秘密鍵を暗号モジュールに格納する手順を記述する。 ※官職証明書の秘密鍵を暗号モジュールに格納する手順について記述する。 ※他の鍵ペアを生成する場合は、その秘密鍵を暗号モジュールに格納する手順について記述する。</p>
<p>6.2.7 秘密鍵の活性化方法</p> <p>(1)CA鍵 CA秘密鍵は、複数人の[IA操作員により管理鍵を用いて]活性化する。</p> <p>(2)[官職]証明書鍵 [官職証明書の秘密鍵は、官職証明書の管理者によりPIN(Personal Identification Number)を用いて活性化する。]</p>	A	<p>※秘密鍵の活性化方法について記述する。 ※他の鍵ペアを生成する場合は、その秘密鍵の活性化方法を記述する。</p>
<p>6.2.8 秘密鍵の非活性化方法</p> <p>(1)CA鍵 CA秘密鍵は、複数人の[IA操作員により管理鍵を用いて]非活性化する。</p> <p>(2)[官職]証明書鍵 [官職証明書の秘密鍵は、官職証明書の管理者によりPINを用いて非活性化する。]</p>	A	<p>※秘密鍵の非活性化方法について記述する。 ※他の鍵ペアを生成する場合は、その秘密鍵の非活性化方法を記述する。</p>

記述内容	区分	備考
<p>6.2.9 秘密鍵の破棄方法</p> <p>(1)CA鍵 HSM内のCA秘密鍵の破棄は、複数人のIA鍵管理者が「HSMを初期化することによって行う。」「なお、初期化したHSMを室外に持ち出す場合は、物理的にHSMを破壊する。」 また、バックアップ媒体内のCA秘密鍵の破棄は、複数人のIA鍵管理者が「媒体を初期化することによって行う。」「なお、初期化したバックアップ媒体を室外へ持ち出す場合は、物理的に媒体を破壊する。」</p> <p>(2)[官職]証明書鍵 [官職証明書の秘密鍵の破棄は、所定の手続に従い破棄する。]</p>	A	<p>※秘密鍵の破棄方法について記述する。 ※HSM内のCA秘密鍵の破棄方法は、少なくともHSMの機能を用いて消去することか、HSMを初期化することのいずれかを記述する。 ※バックアップ媒体内のCA秘密鍵の破棄方法は、少なくとも媒体から消去すること、初期化することのいずれかを記述する。 ※他の鍵ペアを生成する場合は、その秘密鍵の破棄方法を記述する。</p>
<p>6.3 公開鍵の履歴保管と鍵ペアの有効期間</p> <p>6.3.1 公開鍵の履歴保管 公開鍵は証明書のアーカイブに含まれ、「4.6.2 アーカイブデータの保管期間」において定める期間、保管する。</p>	A	<p>※公開鍵の保管期間を記述する。</p>
<p>6.3.2 公開鍵と秘密鍵の有効期間</p> <p>(1)CA鍵 行政機関等CAの公開鍵と秘密鍵の有効期間は、有効とする日から起算して10年とし、5年ごとに鍵更新を行う。 ただし、公開鍵と秘密鍵の有効期間内に行政機関等CAを廃止する場合は、この限りでない。 また、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。</p> <p>(2)[官職]証明書鍵 [官職]証明書の公開鍵と秘密鍵の有効期間は、有効とする日から起算して3年[以下]とする。 ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。</p>	A	<p>※公開鍵及び秘密鍵の有効期間を記述する。 ※他の鍵ペアを生成する場合は、その公開鍵と秘密鍵の有効期間を記述する。</p>
<p>6.4 活性化データ</p> <p>6.4.1 活性化データの生成とインストール</p> <p>(1)CA鍵 [CA秘密鍵を格納するHSMの操作は、パスワードと複数の管理鍵により行う。HSMの操作を行うためのパスワードは、IA鍵管理者が決定しHSMに直接入力する。]</p> <p>(2)[官職]証明書鍵 [官職証明書の秘密鍵を格納するICカードの初期PINは、RA操作員が設定する。]</p>	A	<p>※CA秘密鍵及び官職証明書の秘密鍵の活性化に用いられる活性化データ生成及びインストール方法について記述する。 ※他の鍵ペアを生成する場合は、その活性化データの生成及びインストール方法について記述する。</p>
<p>6.4.2 活性化データの保護</p> <p>(1)CA鍵 [CA秘密鍵を格納するHSMの活性化に必要なパスワードは定期的に変更し、管理鍵は安全に保管する。]</p> <p>(2)[官職]証明書鍵 [官職証明書の秘密鍵を格納するICカードの活性化に必要なPINは定期的に変更し、安全に保管する。]</p>	A	<p>※CA秘密鍵及び官職証明書の秘密鍵の活性化に用いられる活性化データの保護方法について記述する。 ※他の鍵ペアを生成する場合は、その活性化データの保護方法について記述する。</p>
<p>6.5 コンピュータセキュリティ管理</p> <p>6.5.1 コンピュータセキュリティ機能要件</p> <p>行政機関等CAシステムには、アクセス制御機能、操作員の識別と認証機能、[データベースセキュリティのための暗号化機能]、監査ログ及びアーカイブデータの収集機能、CA鍵及びシステムのリカバリ機能等を備える。</p>	A	<p>※行政機関等CAシステムに備えるコンピュータセキュリティ機能について記述する。</p>
<p>6.5.2 コンピュータセキュリティ評価</p> <p>規定しない。</p>	B	<p>※コンピュータのセキュリティについて、準拠する標準を記述する。</p>

記述内容	区分	備考
<p>6. 6 システムのライフサイクルにおけるセキュリティ管理</p> <p>6. 6. 1 システム開発面における管理</p> <p>行政機関等CAのシステム開発、修正又は変更には、所定の手続に基づき、信頼できる組織及び環境下において作業を実施する。開発、修正又は変更したシステムは、[テスト環境]において検証を行い、[行政機関等CA責任者]の承認を得たうえで導入する。また、システム仕様及び検証報告については、文書化し保管する。</p>	A	<p>※行政機関等CAのシステム開発、修正又は変更時におけるセキュリティ管理方法について記述する。</p>
<p>6. 6. 2 システム運用面における管理</p> <p>行政機関等CAのシステムを維持管理するため、OS及びソフトウェアのセキュリティチェックを定期的に行う。また、この検証結果を文書化し保管する。</p>	A	<p>※行政機関等CAのシステム運用時におけるセキュリティ管理方法について記述する。</p>
<p>6. 6. 3 セキュリティ評価の基準</p> <p>規定しない。</p>	B	<p>※セキュリティ管理手続について、準拠する標準を記述する。</p>
<p>6. 7 ネットワークセキュリティ管理</p> <p>行政機関等CAリポジトリに保有する情報のうち公表する情報は、ファイアウォールを介してBCAの統合リポジトリに複製する。</p>	A	<p>※ネットワーク接続の有無、不正アクセス対策等を記述する。</p>
<p>6. 8 暗号モジュールの技術管理</p> <p>「6. 1. 1 鍵ペア生成」及び「6. 2. 1 暗号モジュールに関する基準」において定める。</p>	A	<p>※鍵ペアの生成及び保護に用いる暗号モジュールについて、準拠する標準を記述する。</p>
<p>7. 証明書とCRL/ARLのプロファイル</p>		<p>※行政機関等CAが発行する証明書及びCRL/ARLのプロファイルを記述する。</p>
<p>7. 1 証明書のプロファイル</p>	A	<p>※自己署名証明書、リンク証明書、相互認証証明書、官職証明書等のプロファイルを記述する。なお、証明書の形式は、X.509 v3に従う。</p>
<p>7. 2 CRL/ARLのプロファイル</p>	A	<p>※CRL及びARLのプロファイルを記述する。なお、証明書の形式は、X.509 v2に従う。</p>
<p>8. CP/CPSの管理</p>		<p>※CP/CPSの管理方針について記述する。</p>
<p>8. 1 CP/CPSの変更</p> <p>[行政機関等CA運営委員会]は、本CP/CPSを必要に応じて変更する。</p>	A	<p>※本CP/CPSの変更方針を記述する。</p>
<p>8. 2 CP/CPSの公表と通知</p> <p>[行政機関等CA運営委員会]は、本CP/CPSを変更した場合、速やかに変更したCP/CPSを公表する。これをもって証明書利用者及び証明書検証者への通知とする。</p>	A	<p>※本CP/CPSを変更した場合の公表及び通知方法について記述する。</p>
<p>8. 3 CP/CPSの決定</p> <p>行政機関等CAのCP/CPSは、[行政機関等CA運営委員会]の決定をもって有効なものとする。</p>	A	<p>※本CP/CPSの発効のための手続について記述する。</p>