

証明書ポリシー（CP/CPS）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所		改定理由	論点	対応案	備考
			改定箇所	改定後記載内容				
1	ポリシーの記載修正	CP	1.6 定義と略語	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの <u>金口</u> は「鍵更新」ではなく、新発の鍵発行として扱う。	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの <u>金口</u> は「鍵更新」ではなく、新発の鍵発行として扱う。	山内構成員より鍵ペアが「生成」されるものか「発行」されるものか、表記を統一すべきと指摘を頂いたため	「生成」に記載を統一する。	—
2	ポリシーの記載修正	CP	3.3 鍵更新申請時の本人性確認及び認証	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類 <u>立</u> は記録が無効 <u>立</u> は廃棄されていた場合、証明書の有効期間を <u>金口</u> 若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類若しくは記録が無効 <u>立</u> は廃棄されていた場合、 <u>立</u> は、 <u>立</u> 証明書の有効期間を <u>金口</u> 若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	山内構成員よりわかりやすさ、読みやすさの観点から改定箇所のある文章構造を修正すべきとご指摘を頂いたため	文言の適正化を行う。	—
3	ポリシーの記載修正	CP	9.3.1 秘密情報の範囲	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、いかなる場合でもこれらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、 <u>リモート署名サービスの運営者に対して</u> 、必ず「保健医療福祉分野におけるリモート署名サービスの評価基準」に従い、十分なセキュリティ対策を行うこと。	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、これらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、 <u>リモート署名サービスの運営者に対して</u> 、必ず「保健医療福祉分野におけるリモート署名サービスの評価基準」に従い、十分なセキュリティ対策を行う <u>よう要すること</u> 。	山内構成員より「十分なセキュリティ対策を行う」主体が明らかになるよう記載を修正すべきとご指摘を頂いたため	主体が明らかとなるよう、「リモート署名サービスの運営者に対して、（略）十分なセキュリティ対策を行うよう要求すること。」とする。	—
4	ポリシーの記載修正	CP	1.5.2 問合せ先	【問合せ先】 窓口：厚生労働省 <u>医政局 参事官（医療情報担当）付医療情報連携担当参事官</u>	【問合せ先】 窓口：厚生労働省 <u>政策統括官（情報政策担当）付医療情報連携担当参事官</u>	組織名の変更のため	「医政局 参事官（医療情報担当）付医療情報室」を「政策統括官（情報政策担当）付医療情報連携担当参事官室」に変更する。	—

証明書ポリシー（CP/CPS）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所		改定理由	論点	対応案	備考
			改定前	改定後記載内容				
1	ポリシーの記載修正	CP	1.6 定義と略語	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの置換は「鍵更新」ではなく、新発の鍵発行として扱う。	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの置換は「鍵更新」ではなく、新発の鍵発行として扱う。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
2	ポリシーの記載修正	CP	3.3 鍵更新申請時の本人性確認及び認証	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類若しくは記録が無効又は廃棄されていた場合、証明書の有効期間を過ぎた後若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類若しくは記録が無効又は廃棄されていた場合、証明書の有効期間を過ぎた後若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
3	ポリシーの記載修正	CP	9.3.1 秘密情報の範囲	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、いかなる場合でもこれらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、必ず『保健医療福祉分野におけるリモート署名サービスの評価基準』に従い、十分なセキュリティ対策を行うこと。	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、これらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、リモート署名サービスの運営者に対して、必ず『保健医療福祉分野におけるリモート署名サービスの評価基準』に従い、十分なセキュリティ対策を行うよう要すること。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
4	ポリシーの記載修正	CP	1.5.2 問合せ先	【問合せ先】 窓口：厚生労働省 医政局 参事官（医療情報担当）付医療情報課 ※	【問合せ先】 窓口：厚生労働省 政策統括官（情報政策担当）付医療情報課 担当参事官※	組織名の変更のため	CP（署名用）と同じ記載に変更する。	－

証明書ポリシー（CP/CPS）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所		改定理由	論点	対応案	備考
			改定前	改定後記載内容				
1	ポリシーの記載修正	CP	1.6 定義と略語	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期間を過ぎた後に行われる鍵ペアの置換は「鍵更新」ではなく、新発の鍵発行として扱う。	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期間を過ぎた後に行われる鍵ペアの置換は「鍵更新」ではなく、新発の鍵発行として扱う。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
2	ポリシーの記載修正	CP	3.3 鍵更新申請時の本人性確認及び認証	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類若しくは記録が無効又は廃棄されていた場合、証明書の有効期間を過ぎた後若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	ただし、前回の更新を「3.2.3 個人の認証」で提出した書類若しくは認証局で作成された記録を再び参照することにより行った場合、元の書類若しくは記録が無効又は廃棄されていた場合、証明書の有効期間を過ぎた後若しくは証明書が失効した場合は、「3.2.3 個人の認証」に定める手続きにより申請するものとする。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
3	ポリシーの記載修正	CP	9.3.1 秘密情報の範囲	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、いかなる場合でもこれらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、必ず「保健医療福祉分野におけるリモート署名サービスの評価基準」に従い、十分なセキュリティ対策を行うこと。	加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、これらの鍵へのアクセス手段を提供しない。ただし、リモート署名サービスの利用に伴い私有鍵にアクセスする必要がある場合は、リモート署名サービスの運営者に対して、必ず「保健医療福祉分野におけるリモート署名サービスの評価基準」に従い、十分なセキュリティ対策を行うよう要すること。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	－
4	ポリシーの記載修正	CP	1.5.2 問合せ先	【問合せ先】 窓口：厚生労働省 医政局 参事官（医療情報担当）付医療情報課 ※	【問合せ先】 窓口：厚生労働省 政策統括官（情報政策担当）付医療情報課 担当参事官※	組織名の変更のため	CP（署名用）と同じ記載に変更する。	－

証明書ポリシー（CP/CPS）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所		改定理由	論点	対応案	備考	
			改定項番	記載内容					
1	ポリシーの記載修正	CP	1.6 定義と略語	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの <u>金証</u> は「鍵更新」ではなく、新規の鍵発行として扱う。	・鍵更新（Key Update） 認証局が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。本CPでは、有効期限前に実施される鍵ペアの置換を「鍵更新」と定義し、有効期限を過ぎた後に行われる鍵ペアの <u>金証</u> は「鍵更新」ではなく、新規の鍵発行として扱う。	CP（署名用）の記載との整合性を確保するため	CP（署名用）と同じ記載に変更する。	—	
2	ポリシーの記載修正	CP	1.3.2 登録局	本認証局では、厚生労働省 <u>医政局</u> 、 <u>参事官</u> 、 <u>医療情報担当</u> 、 <u>付医療情報担当</u> が登録局の役割を担うこととする。	本認証局では、厚生労働省 <u>政策統括官</u> 、 <u>情報政策担当</u> 、 <u>付医療情報連携担当</u> 、 <u>参事官</u> が登録局の役割を担うこととする。	組織名の変更のため	—	「医政局 参事官（医療情報担当）付医療情報室」を「政策統括官（情報政策担当）付医療情報連携担当参事官室」に変更する。	—
3	ポリシーの記載修正	CP	1.3.3 加入者	加入者とは、厚生労働省 <u>医政局</u> 、 <u>参事官</u> 、 <u>医療情報担当</u> 、 <u>付医療情報連携担当</u> からサブCAの運用業務の実施を承認された組織であり、署名用サブCA証明書、認証用（人）サブCA証明書の証明書所有者である（以下、「署名用サブCA証明書と認証用（人）サブCA証明書の全てを意味する場合はサブCA証明書」と呼ぶ。）。	加入者とは、厚生労働省 <u>政策統括官</u> 、 <u>情報政策担当</u> 、 <u>付医療情報連携担当</u> 、 <u>参事官</u> からサブCAの運用業務の実施を承認された組織であり、署名用サブCA証明書、認証用（人）サブCA証明書の証明書所有者である（以下、「署名用サブCA証明書と認証用（人）サブCA証明書の全てを意味する場合はサブCA証明書」と呼ぶ。）。	組織名の変更のため	—	「医政局 参事官（医療情報担当）付医療情報室」を「政策統括官（情報政策担当）付医療情報連携担当参事官室」に変更する。	—
4	ポリシーの記載修正	CP	1.5.2 問合せ先	【問合せ先】 窓口：厚生労働省 <u>医政局</u> 、 <u>参事官</u> 、 <u>医療情報担当</u> 、 <u>付医療情報連携担当</u>	【問合せ先】 窓口：厚生労働省 <u>政策統括官</u> 、 <u>情報政策担当</u> 、 <u>付医療情報連携担当参事官室</u>	組織名の変更のため	—	CP（署名用）と同じ記載に変更する。	—

準拠性監査様式（署名用）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所			改定理由	論点	対応案	備考
			改定項番	記載内容	改定後記載内容				
1	CP更新に伴う更新	保健医療福祉分野PKI認証局証明書ポリシ準拠性監査報告書様式（署名用）	－	－	－	CPの更新に伴い、準拠性監査様式へCP内の更新箇所を反映するため	－	CP内の更新箇所を反映する。	－

準拠性監査様式（認証用）に関する改定検討箇所と対応案

No.	分類	対象	改定箇所			改定理由	論点	対応案	備考
			改定項番	記載内容	改定後記載内容				
1	CP更新に伴う更新	保健医療福祉分野PKI認証局証明書ポリシ準拠性監査報告書様式（認証用）	－	－	－	CPの更新に伴い、準拠性監査様式へCP内の更新箇所を反映するため	－	CP内の更新箇所を反映する。	－

準拠性審査手続規則に関する改定検討箇所と対応案

No.	分類	対象	改定箇所			改定理由	論点	対応案	備考
			改定項番	記載内容	改定後記載内容				
1	記載修正	準拠性審査手続規則	第 1 条	本規則は、厚生労働省 <u>大臣官房医薬産業振興・医療情報審査課</u> が開催する「保健医療福祉分野における公同健基盤認証局の整備と運営に関する専門家会議」が行う保健医療福祉分野 P K I 認証局証明書ポリシー（以下「C P」という。）および保健医療福祉分野におけるリモート署名サービス評価基準への準拠性審査、CA鍵の更新の手順について必要な事項を定めることにより、準拠性審査の円滑な遂行を図ることを目的とする。	本規則は、厚生労働省 <u>政策統括官（情報政策担当）</u> が開催する「保健医療福祉分野における公同健基盤認証局の整備と運営に関する専門家会議」が行う保健医療福祉分野 P K I 認証局証明書ポリシー（以下「C P」という。）および保健医療福祉分野におけるリモート署名サービス評価基準への準拠性審査、CA鍵の更新の手順について必要な事項を定めることにより、準拠性審査の円滑な遂行を図ることを目的とする。	組織名の変更のため	－	「大臣官房医薬産業振興・医療情報審査課」を「政策統括官（情報政策担当）」に変更する。	－
2	記載修正	準拠性審査手続規則	第 2 条第四号	厚生労働省 <u>大臣官房医薬産業振興・医療情報審査課</u> が開催する「保健医療福祉分野における公同健基盤認証局の整備と運営に関する専門家会議」をいう。	厚生労働省 <u>政策統括官（情報政策担当）</u> が開催する「保健医療福祉分野における公同健基盤認証局の整備と運営に関する専門家会議」をいう。	組織名の変更のため	－	「大臣官房医薬産業振興・医療情報審査課」を「政策統括官（情報政策担当）」に変更する。	－
3	記載修正	準拠性審査手続規則	第 2 条第五号	厚生労働省 <u>医政局参事官（医療情報担当）付医療情報室</u> に設置されている申請認証局、申請 T S P からの申請を受け付ける部門をいう。	厚生労働省 <u>政策統括官（情報政策担当）付医療情報連携担当参事官室</u> に設置されている申請認証局、申請 T S P からの申請を受け付ける部門をいう。	組織名の変更のため	－	「医政局 参事官（医療情報担当）付医療情報室（情報政策担当）付医療情報連携担当参事官室」に変更する。	－
4	記載修正	準拠性審査手続規則	別紙 1－1	<u>審議官（※）へ答申</u> <u>（※）大臣官房医薬産業振興・医療情報審査課</u>	<u>政策統括官（情報政策担当）へ答申</u>	組織名の変更のため	－	「政策統括官（情報政策担当）へ答申」に修正する。	－
5	記載修正	準拠性審査手続規則	別紙 1－2	<u>審議官（※）へ答申</u> <u>（※）大臣官房医薬産業振興・医療情報審査課</u>	<u>政策統括官（情報政策担当）へ答申</u>	組織名の変更のため	－	「政策統括官（情報政策担当）へ答申」に修正する。	－
6	記載修正	準拠性審査手続規則	別紙 1－3	<u>審議官（※）へ答申</u> <u>（※）大臣官房医薬産業振興・医療情報審査課</u>	<u>政策統括官（情報政策担当）へ答申</u>	組織名の変更のため	－	「政策統括官（情報政策担当）へ答申」に修正する。	－

準拠性審査実施規則に関する改定検討箇所と対応案

No.	分類	対象	改定箇所			改定理由	論点	対応案	備考
			改定項番	記載内容	改定後記載内容				
1	記載修正	準拠性審査実施規則	第1条	第1条本規則は、厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> が開催する「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以下「専門家会議」という。）が行う保健医療福祉分野P K I 認証局証明書ポリシーおよび保健医療福祉分野におけるリモート署名サービス評価基準への準拠性審査を実施するために必要な事項を定めることにより、準拠性審査の円滑な遂行を図ることを目的とする。	第1条本規則は、厚生労働省 <u>政策統括官（情報政策担当）</u> が開催する「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以下「専門家会議」という。）が行う保健医療福祉分野P K I 認証局証明書ポリシーおよび保健医療福祉分野におけるリモート署名サービス評価基準への準拠性審査を実施するために必要な事項を定めることにより、準拠性審査の円滑な遂行を図ることを目的とする。	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
2	記載修正	準拠性審査実施規則	第2条	第2条申請認証局、申請トラストサービスプロバイダー（以下「申請T S Pという。」）は保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシーの準拠性審査およびこれに伴うキーセレモニー立会、保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査又はCA鍵更新に伴うキーセレモニー立会を受けるために次の書類のうち申請予定項目に該当するものを厚生労働省 <u>医政局参事官（医療情報担当）付医療情報室</u> に提出する。	第2条申請認証局、申請トラストサービスプロバイダー（以下「申請T S Pという。」）は保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシーの準拠性審査およびこれに伴うキーセレモニー立会、保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査又はCA鍵更新に伴うキーセレモニー立会を受けるために次の書類のうち申請予定項目に該当するものを厚生労働省 <u>政策統括官（情報政策担当）付医療情報連携担当参事官室</u> に提出する。	組織名の変更のため	—	「医政局 参事官（医療情報担当）付医療情報室」を「政策統括官（情報政策担当）付医療情報連携担当参事官室」に変更する。	—
3	記載修正	準拠性審査実施規則	第6条	準拠性審査認定の有効期間は2年間とし、申請認証局、申請T S Pは同認定後1年が経過したときあるいは準拠性に関連する変更を行った場合は速やかに監査報告書を厚生労働省 <u>医政局参事官（医療情報担当）付医療情報室</u> に提出する。	準拠性審査認定の有効期間は2年間とし、申請認証局、申請T S Pは同認定後1年が経過したときあるいは準拠性に関連する変更を行った場合は速やかに監査報告書を厚生労働省 <u>政策統括官（情報政策担当）付医療情報連携担当参事官室</u> に提出する。	組織名の変更のため	—	「医政局 参事官（医療情報担当）付医療情報室（情報政策担当）付医療情報連携担当参事官室」に変更する。	—
4	記載修正	準拠性審査実施規則	第7条	申請認証局、申請T S Pが更新を希望する場合の準拠性審査の手続については、手続規則に準じて行うものとし、認定後1年から1年6月の期間に第2条及び第3条に定める申請書類等を厚生労働省 <u>医政局参事官（医療情報担当）付医療情報室</u> に提出するものとする。	申請認証局、申請T S Pが更新を希望する場合の準拠性審査の手続については、手続規則に準じて行うものとし、認定後1年から1年6月の期間に第2条及び第3条に定める申請書類等を厚生労働省 <u>政策統括官（情報政策担当）付医療情報連携担当参事官室</u> に提出するものとする。	組織名の変更のため	—	「医政局 参事官（医療情報担当）付医療情報室（情報政策担当）付医療情報連携担当参事官室」に変更する。	—
5	記載修正	準拠性審査実施規則	第1号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> 、殿	厚生労働省 <u>政策統括官（情報政策担当）</u> 、殿	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
6	記載修正	準拠性審査実施規則	第1号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシー準拠性審査を受けたいので下記のとおり申請します。	厚生労働省 <u>政策統括官（情報政策担当）</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシー準拠性審査を受けたいので下記のとおり申請します。	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
7	記載修正	準拠性審査実施規則	第2号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> 、殿	厚生労働省 <u>政策統括官（情報政策担当）</u> 、殿	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
8	記載修正	準拠性審査実施規則	第2号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査を受けたいので下記のとおり申請します。	厚生労働省 <u>政策統括官（情報政策担当）</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査を受けたいので下記のとおり申請します。	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
9	記載修正	準拠性審査実施規則	第3号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> 、殿	厚生労働省 <u>政策統括官（情報政策担当）</u> 、殿	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—
10	記載修正	準拠性審査実施規則	第3号様式	厚生労働省 <u>大臣官房医産産業振興・医療情報審議会</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシーに規定されるCA鍵の更新を行うため下記のとおり申請します。	厚生労働省 <u>政策統括官（情報政策担当）</u> の「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」が行う保健医療福祉分野P K I 認証局署名用・認証用（人）証明書ポリシーに規定されるCA鍵の更新を行うため下記のとおり申請します。	組織名の変更のため	—	「大臣官房医産産業振興・医療情報審議会」を「政策統括官（情報政策担当）」に変更する。	—

証明書ポリシ（CP/CPS）に関する改訂検討箇所と対応案

[illegible]

[illegible]

[illegible]

資料1-2-3
証明書ポリシー（CP/CP5）に関する改訂検討箇所と対応案

No.	項目	内容	改訂箇所	改訂理由	対応策	備考	対応策	備考	
1	ポリシーの記載修正	CP	1.6 更新と検証	「更新前 (Pre-update)」 更新前が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。鍵ペアは、有効期限内に生成された鍵ペアの置き換えを指す。鍵ペアは、 「更新前」と変更し 、有効期限を過ぎた後に生成した鍵ペアの取り扱いは「更新前」ではなく、秘密鍵の破棄行為として扱う。	「更新前 (Pre-update)」 更新前が生成した鍵ペアを、新しい鍵ペアへ置き換える行為を指す。鍵ペアは、 「更新前」と変更し 、有効期限を過ぎた後に生成した鍵ペアの取り扱いは「更新前」ではなく、秘密鍵の破棄行為として扱う。	「有効期限」の変更は「有効期限及び山内構成要素からの指摘を踏まえて、記載を修正	—	「有効期限」の記載を「有効期限」を使用した表現に変更する。	—
2	ポリシーの記載修正	CP	1.6 更新と検証	「更新前 (Pre-update)」 「更新前」に、何らかの理由（盗難・紛失など）により電子証明書を取り消すこと、盗失の防止、本人からの申請によるが、更新後に生成した証明書が提供されることもある。	「更新前」に、何らかの理由（盗難・紛失など）により電子証明書を取り消すこと、盗失の防止、本人からの申請によるが、更新後に生成した証明書が提供されることもある。	六川構成員及び山内構成要素からの指摘を踏まえて、記載を修正	—	「有効期限」の記載を「有効期限」を使用した表現に変更する。	—
3	ポリシーの記載修正	CP	1.6 更新と検証	更新と検証	「更新前」に、何らかの理由（盗難・紛失など）により電子証明書を取り消すこと、盗失の防止、本人からの申請によるが、更新後に生成した証明書が提供されることもある。	「有効期限」と合わせて、「使用期限」の記載を追加	—	鍵ペアの「使用期限」について、変更を追加する。	—
4	ポリシーの記載修正	CP	1.6 更新と検証	更新と検証	「有効期限 (Validity Period)」 証明書が生成された日からとられる期間であり、 有効期限満後も有効期間終了日まで有効性を保つ	CP内「1.6 更新と検証」へ証明書の「有効期限」と「有効期限」が併列しているのを、変更を追加する。	—	—	—
5	ポリシーの記載修正	CP	4.7.1 証明書更新要求の要件	証明書は、以下の条件を満たす時に証明書の更新申請を受け付ける。なお、更新申請期間中に証明書の更新申請の期限の満了日が経過した場合は、更新申請期間が満了したものと見なす。 ・更新申請期間中に証明書の更新申請が満了したものであること。 ・証明書の有効期限が満了したものであること。 ・更新申請が満了したものであること。 ・更新申請が満了したものであること。	証明書は、以下の条件を満たす時に証明書の更新申請を受け付ける。なお、更新申請期間中に証明書の更新申請の期限の満了日が経過した場合は、更新申請期間が満了したものと見なす。 ・更新申請期間中に証明書の更新申請が満了したものであること。 ・証明書の有効期限が満了したものであること。 ・更新申請が満了したものであること。 ・更新申請が満了したものであること。	六川構成員及び山内構成要素からの指摘を踏まえて、記載を修正	—	CP内「4.7.1 証明書更新要求の要件」の文言について、有効期限内のものをあれば更新可能である文言へ修正する。	—
6	ポリシーの記載修正	CP	4.2.1 番号セ珍妮の形式及び管理	ルートCA5有数の機密番号は、US FIPS 140-2 レベル3又は US FIPS 140-3 レベル3と同等以上の規格に準拠するものとする。	ルートCA5有数の機密番号は、US FIPS 140-2 レベル3又は US FIPS 140-3 レベル3と同等以上の規格に準拠するものとする。	根本部長からの指摘を踏まえて、記載を修正	—	FIPS140-2と140-3の併記の扱いについて、140-2は前掲付きであることを見直すよう修正する。 また、日本国政府の公的署名オペレータからいただいたご意見を踏まえて、「併記以上の規格に準拠」ではなく、「併記以上のものを参照する」と記載を修正する。添えて、 もともとの11で記載を踏まえる	—
7	ポリシーの記載修正	CP	4.2.1.1 番号セ珍妮の形式	ルートCA5有数の機密番号は、FIPS 140-2 レベル3又は FIPS 140-3 レベル3と同等以上のものを参照するものとする。	ルートCA5有数の機密番号は、FIPS 140-2 レベル3又は US FIPS 140-3 レベル3と同等以上のものを参照するものとする。	根本部長からの指摘を踏まえて、記載を修正	—	—	—
8	ポリシーの記載修正	CP	4.3.2 公開鍵証明書の有効期限と鍵ペアの有効期限	公開鍵証明書は、 「更新前」の期間 については、 第6-3に示す 。	公開鍵証明書は、 「更新前」の期間 については、 第6-3に示す 。 ・公開鍵は「有効期限」という概念がないため、 「更新前」の期間 と記載を修正	第5.1.1.1の鍵ペアを記載されているのに対し、文中中では公開鍵と記載されているため、整合性を合わせる。また、鍵ペアは「有効期限」という概念がないため、 「更新前」の期間 と記載を修正	—	「有効期限」を「更新前」に変更する。 鍵の有効期限を公開鍵期間、鍵ペアの期限とする。 鍵ペアについて、「有効期限」という記載を使用しないように記載を修正する。	—
9	ポリシーの記載修正	CP	4.6.4 検証者の条件	「証明書の有効期限が満了していないこと」	「証明書の有効期限が満了していないこと」	六川構成員及び山内構成要素からの指摘を踏まえて、記載を修正	—	「有効期限」の記載を「有効期限」を使用した表現に変更する。	—

[illegible]

証明書ポリシ（CP/CPS）に関する改訂検討箇所と対応案

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

証明書ポリシ（CP/CPS）に関する改訂検討箇所と対応策

[illegible]

証明書ポリシ（CP/CPS）に関する改訂検討箇所と対応案

[illegible]

[illegible]

[illegible]

資料1-2-1
証明書ポリシ（CP/CPS）に関する改訂検討箇所と対応案

[illegible]

[illegible]

準拠性監査様式（署名用、認証用）に関する改訂検討箇所と対応案

No.	分類	対象	改訂箇所			改訂理由	論点	対応案	備考
			改訂項番	記載内容	改訂後記載内容				
1	CP更新に伴う更新	保健医療福祉分野PKI認証局証明書ポリシ準拠性監査報告書様式（署名用）	－	－	－	CPの更新に伴い、準拠性監査様式へCP内の更新箇所を反映する。	－	更新箇所の反映。	－
2	CP更新に伴う更新	保健医療福祉分野PKI認証局証明書ポリシ準拠性監査報告書様式（認証用）	－	－	－	CPの更新に伴い、準拠性監査様式へCP内の更新箇所を反映する。	－	更新箇所の反映。	－

準拠性審査手続規則・実施規則に関する改訂検討箇所と対応案

No.	分類	対象	改訂箇所			改訂理由	論点	対応案	備考
			改訂対象	記載内容	改訂後記載内容				
1	準拠性審査手続規則・実施規則の修正	準拠性審査手続規則	別紙2 準拠性審査 実地調査手順	1. 代表者インタビュー 組織概要/業務内容/経営方針 申請のきっかけ 管理者・監査責任者の任命プロセス、任命記録の確認 マネジメントレビュー（組織のガバナンス体制）	1. 代表者インタビュー 組織概要/業務内容/経営方針 申請のきっかけ 管理者・監査責任者の任命プロセス、任命記録の確認 マネジメントレビュー（組織のガバナンス体制） <u>※代表者：ISO/IEC 27001（ISMS）の規格に基づき、方針や目標の策定・調整、統制などを行う権限を持つ、組織内で最上位に位置する個人、またはグループで構成されるトップマネジメントを指す。</u>	現状の記載では代表者の定義がされておらず、実地調査の際、誰を対象にインタビューをすればよいのかわからないため。	実地調査での代表者インタビューについて、対象となる「代表者」の定義がされていないため、審査人が正確なインタビューを実施できず、適切な情報を得ることができないのではないか。	代表者が誰を指すのか、定義を追記する。 ⇒ISO27001（ISMS）の定義されている組織のトップマネジメントを想定。	—
2	記載修正	準拠性審査手続規則	別紙2 準拠性審査 実地調査手順	3. 実地確認 人的セキュリティの確認（管理方針の周知、教育、等） 物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	3. 実地確認 人的セキュリティの確認（管理方針の周知、教育、等） 物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	他の文面と比べて平仄があわないため。	—	漏えいに記述を揃える。	—
3	記載修正	準拠性審査手続規則	別紙4-1 保健医療福祉分野PKI認証局証明書ポリン準拠性審査記録	物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	他の文面と比べて平仄があわないため。	—	漏えいに記述を揃える。	—
4	記載修正	準拠性審査手続規則	別紙4-2 保健医療福祉分野におけるリモート署名サービス評価基準準拠性審査記録	物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	物理セキュリティの確認（入退管理、鍵管理、 <u>漏えい</u> 対策、等）	他の文面と比べて平仄があわないため。	—	漏えいに記述を揃える。	—