

厚生労働省 HPKI ルート認証局運用管理規程の改訂論点

令和 2 年 9 月 16 日
厚生労働省
医政局研究開発振興課
医療情報技術推進室

現行規程：厚生労働省 HPKI ルート認証局 Ver1.1 （平成 25 年 9 月 1 日、厚生労働省）

https://www.mhlw.go.jp/content/10808000/MHLW-CPCPS_Ver1.1.pdf

改訂論点について以下①及び②に示す。

① 1.5.2 問い合わせ先等の修正

2018 年 10 月に厚労省内の HPKI ルート認証局に関する所掌が政策統括官から医政局に移管したが、その点について改訂されていなかったため、問い合わせを修正する。修正箇所を表 1 に示す。

表 1. 論点①の該当項目の新旧

改訂案	現行：厚生労働省 HPKI ルート認証局 Ver1.1
<p>1.3.2 登録局</p> <p>本認証局では、厚生労働省 <u>医政局 研究開発振興課医療情報技術推進室</u>が登録局の役割を担うこととする。</p> <p>登録局は、適切な申請者の組織確認の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効</p>	<p>1.3.2 登録局</p> <p>本認証局では、厚生労働省 <u>政策統括官付 情報政策担当参事官室</u>が登録局の役割を担うこととする。</p> <p>登録局は、適切な申請者の組織確認の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を</p>

を含む。

但し、登録局は本 CP/CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部を外部に委託することができる。

1.3.3 加入者

加入者とは、厚生労働省 医政局 研究開発振興課医療情報技術推進室 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。）。サブ CA 証明書所有者の範囲は次のとおりとする。

- ・ 保健医療福祉分野サービスの提供者

1.5.2 問い合わせ先

本 CP/CPS に関する問い合わせ先を以下のように定める。

【問い合わせ先】

窓口：厚生労働省 医政局 研究開発振興課医療情報技術推進室

（以下、「厚生労働省」と呼ぶ。）

含む。

但し、登録局は本 CP/CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部を外部に委託することができる。

1.3.3 加入者

加入者とは、厚生労働省 政策統括官付 情報政策担当参事官室 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。）。サブ CA 証明書所有者の範囲は次のとおりとする。

- ・ 保健医療福祉分野サービスの提供者

1.5.2 問い合わせ先

本 CP/CPS に関する問い合わせ先を以下のように定める。

【問い合わせ先】

窓口：厚生労働省 政策統括官付 情報政策担当参事官室
（以下、「厚生労働省」と呼ぶ。）

受付時間：10時～17時

電話番号：[03-3595-2430](tel:03-3595-2430)

FAX 番号：[03-3503-0595](tel:03-3503-0595)

e-mail アドレス：hpki-cp@mhlw.go.jp

受付時間：10時～17時

電話番号：[03-3595-2314](tel:03-3595-2314)

FAX 番号：[03-3595-2198](tel:03-3595-2198)

e-mail アドレス：hpki-cp@mhlw.go.jp

② 4.4.2 認証局による証明書の公開等の訂正

現行ルート CP/CPS では、サブ CA の公開鍵証明書をリポジトリにて公開することとなっている。しかしサブ CA の公開鍵証明書をルートとサブ両方で公開することは、サブ CA の加入者に混乱を招きかねない。CP の記載も「CA の公開鍵証明書」とのみ記載されており、これは CA 自身の公開鍵証明書と理解しサブ CA の公開鍵証明書は含まないと理解し、ルート CP/CPS からサブ CA の公開鍵証明書の公表を削除する。

なお、現在は、リポジトリ（※1）にて各サブ CA の HP リンクを指定し、そこに問い合わせるよう記載したことをもって、サブ CA の公開鍵証明書を公開していることとしている。

（※1）HPKI 認証局運用規約関連資料・証明書類

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/repository.html

また、本認証局（ルート認証局）にて公開することとなっている「検証者同意書」「利用者同意書」について、「同意書」といった文書はなく、CP 上の「検証者の表明保証に関する文書」「認証局の定める加入者に関する各種規程/基準」は、ルート CP/CPS 上の規程（9.6.4 検証者の表明保証、9.6.3 加入者の表明保証）で示している。そのため、その旨が明確になるよう改訂する。

修正箇所及び当該箇所の CP の対比を表 2 に示す。

表 2. 論点②の該当項目の新旧及び CP の該当箇所

改訂案	現行：厚生労働省 HPKI ルート認証局 Ver1.1	保健医療福祉分野 PKI 認証局 署名用証明書ポリシ 1.5 .1 版
2 公開及びリポジトリの責任	2 公開及びリポジトリの責任	2 公開及びリポジトリの責任
2.1 リポジトリ	2.1 リポジトリ	2.1 リポジトリ

リポジトリはルート CA の証明書と失効情報及びサブ CA の失効情報、その他、保険医療福祉分野 PKI に関する情報を保持する。

2.2 証明書情報の公開

本認証局は、以下の情報を検証者と加入者が入手可能にする。

< 検証者に公開する事項 >

- ・ ルート CA の公開鍵証明書
- ・ 本 CP/CPS
- ・ CRL/ARL
- ・ 検証者の表明保証に関する事項（本 CP/CPS 「9.6.4 検証者の表明保証」に規定する）

< 加入者に公開する事項 >

- ・ 本 CP/CPS
- ・ 利用者の表明保証に関する事項同意書（本 CP/CPS 「9.6.3 加入者の表明保証」に規定する）

リポジトリはルート CA の証明書と失効情報及びサブ CA の証明書と失効情報、その他、保険医療福祉分野 PKI に関する情報を保持する。

2.2 証明書情報の公開

本認証局は、以下の情報を検証者と加入者が入手可能にする。

< 検証者に公開する事項 >

- ・ ルート CA の公開鍵証明書
- ・ サブ CA の公開鍵証明書
- ・ 本 CP/CPS
- ・ CRL/ARL
- ・ 検証者同意書

< 加入者に公開する事項 >

- ・ 本 CP/CPS
- ・ 利用者同意書

リポジトリは認証局の証明書と失効情報及び加入者の失効情報を保持する。

2.2 証明書情報の公開

認証局は、以下の情報を検証者と加入者が入手可能にする。

< 検証者に公開する事項 >

- ・ CA の公開鍵証明書
- ・ 本 CP
- ・ CRL/ARL
- ・ 検証者の表明保証に関する文書

< 加入者に公開する事項 >

- ・ 認証局の定める CPS
- ・ 認証局の定める加入者に関する各種規程 / 基準

2.3 公開の時期又はその頻度

認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CP/CPS「4.9 証明書の失効と一時停止」に従うものとする。

2.4 リポジトリへのアクセス管理

本 CP/CPS、ルート CA 証明書及び [CRL/ARL](#) などの公開情報は、加入者及び検証者に対しては読み取り専用として公開する。

4.1.2 申請手続及び責任

厚生労働省からサブ CA の運用業務を認められた組織は、所定の手続きに基づき、認証局の定める書類及び証明書発行要求 (CSR) を提出することによりサブ CA 証明書の利用申請を行う。

2.3 公開の時期又はその頻度

認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CP/CPS「4.9 証明書の失効と一時停止」に従うものとする。

2.4 リポジトリへのアクセス管理

本 CP/CPS、ルート CA 証明書、サブ CA 証明書及びそれらの証明書の現在の状態などの公開情報は、加入者及び検証者に対しては読み取り専用として公開する。

4.1.2 申請手続及び責任

厚生労働省からサブ CA の運用業務を認められた組織は、所定の手続きに基づき、認証局の定める書類及び証明書発行要求 (CSR) を提出することによりサブ CA 証明書の利用申請を行う。

2.3 公開の時期又はその頻度

認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CP「4.9 証明書の失効と一時停止」に従うものとする。

2.4 リポジトリへのアクセス管理

CP、CPS、証明書及びそれらの証明書の現在の状態などの公開情報は、加入者及び検証者に対しては読み取り専用として公開する。

4.1.2 申請手続及び責任

証明書の利用を希望する者は、認証局で定める以下のいずれかの手続きによって証明書の利用申請を行う。

1. 持参もしくは交付時に本人が出頭する場合

<p>また、サブ CA の運用業務を認められた組織は、申請にあたり、本 CP/CPS「1.3 PKI の適用範囲」と第 9 章で規定される認証局の責任範囲 <u>及び加入者の表明保証の内容</u> を理解し、それらに同意した上で利用申請を行うものとする。</p>	<p>また、サブ CA の運用業務を認められた組織は、申請にあたり、本 CP/CPS「1.3 PKI の適用範囲」と第 9 章で規定される認証局の責任範囲 <u>を理解し、また、利用者同意書も利用申請の前に読み、内容を理解し、それらに同意した上で利用申請を行うものとする。</u></p>	<p>(省略)</p> <p>2. 郵送 (省略)</p> <p>3. オンライン (省略)</p> <p>また、証明書の利用申請者は、申請にあたり、本 CP「1.3 PKI の関係者」と第 9 章で規定される認証局の責任範囲を理解し、同意した上で利用申請を行うものとする。更に、本 CP に則り運営される、各認証局の定める開示文書及び利用約款等も利用申請の前に読み、内容を理解し、それらに読み、内容を理解し、それらに同意した上で利用申請を行うものとする。</p>
<p>4.4.2 認証局による証明書の公開</p>	<p>4.4.2 認証局による証明書の公開</p>	<p>4.4.2 認証局による証明書の公開</p>
<p>認証局は、サブ CA 証明書をリポジトリにて公開 <u>しない</u>。</p>	<p>認証局は、サブ CA 証明書をリポジトリにて公開 <u>する</u>。</p>	<p>認証局は、加入者の署名用証明書の公開を行わない。</p>
<p>4.7.6 認証局による鍵更新証明書の公開</p>	<p>4.7.6 認証局による鍵更新証明書の公開</p>	<p>4.7.6 認証局による鍵更新証明書の公開</p>
<p>認証局は、サブ CA 証明書をリポジトリにて公開 <u>しない</u>。</p>	<p>認証局は、サブ CA 証明書をリポジトリにて公開 <u>する</u>。</p>	<p>認証局は署名用証明書の公開を行わない。</p>

9.6.3 加入者の表明保証

加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任
(省略)
2. 証明書記載事項の担保責任
(省略)
3. 鍵などの管理責任
(省略)
4. 各種の届出に対する責任
(省略)
5. 利用規定の遵守責任

加入者は、本 CP/CPS 及び本項を読み、その利用規定及び禁止規定を遵守すること。

9.6.4 検証者の表明保証

検証者は以下の責任を果たすものとする。

9.6.3 加入者の表明保証

加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任
(省略)
2. 証明書記載事項の担保責任
(省略)
3. 鍵などの管理責任
(省略)
4. 各種の届出に対する責任
(省略)
5. 利用規定の遵守責任

加入者は、本 CP/CPS 及び利用者同意書を読み、その利用規定及び禁止規定を遵守すること。

9.6.4 検証者の表明保証

検証者は以下の責任を果たすものとする。

9.6.3 加入者の表明保証

本 CP に則り運営される認証局の加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任
(省略)
2. 証明書記載事項の担保責任
(省略)
3. 鍵などの管理責任
(省略)
4. 各種の届出に対する責任
(省略)
5. 利用規定の遵守責任

加入者は、本 CP 及び認証局で加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。

9.6.4 検証者の表明保証

本 CP に則り運営される認証局の検証者は以

<p>る。</p> <p>1. 利用規定の遵守責任 検証者は、本 CP/CPS 及び本項を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実にすること。</p> <p>2. 証明書記載事項の確認責任 (省略)</p>	<p>る。</p> <p>1. 利用規定の遵守責任 検証者は、本 CP/CPS 及び<u>検証者同意書</u>を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実にすること。</p> <p>2. 証明書記載事項の確認責任 (省略)</p>	<p>下の責任を果たすものとする。</p> <p>1. 利用規定の遵守責任 検証者は、本 CP 及び認証局で検証者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実にすること。</p> <p>2. 証明書記載事項の確認責任 (省略)</p>
---------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

参照文書

・ HPKI 認証局署名用証明書ポリシー 1.5.1 版 (平成 31 年 4 月、厚生労働省)

<https://www.mhlw.go.jp/content/000508449.pdf>

以上