平成１８年３月３１日
行政情報化推進会議決定

厚生労働省認証局運用管理要綱（ＣＰ／ＣＰＳ ）

厚生労働省認証局運営委員会

目 次

１.はじめに

厚生労働省認証局運用管理要綱（以下「本ＣＰ／ＣＰＳ」という。）は、国民等と厚生労働省との間の申請・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と相互認証を行い官職の証明書等を発行する厚生労働省認証局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。

１．１ 概要

厚生労働省認証局は、官職に対して官職証明書を発行し、業務サーバ等に対してサーバ証明書を発行し、その他厚生労働省認証局の運用に必要な証明書を発行するとともに、ブリッジ認証局と相互認証証明書を取り交わす。

厚生労働省認証局は、証明書ポリシ及び認証実施規定をそれぞれ独立したものとせず、本ＣＰ／ＣＰＳを厚生労働省認証局の認証業務に関する運営方針として位置付ける。

１．２ 識別

厚生労働省認証局の証明書ポリシの識別子は、次のとおりとする。

厚生労働省認証局相互認証証明書ポリシ：1.2.392.100495.8.5.1.1.10
厚生労働省認証局相互認証テスト用証明書ポリシ：1.2.392.100495.8.5.1.1.0
厚生労働省認証局官職証明書ポリシ：1.2.392.100495.8.5.1.1.10
厚生労働省認証局テスト用官職証明書ポリシ：1.2.392.100495.8.5.1.1.0
厚生労働省認証局サーバ証明書ポリシ：規定しない
厚生労働省認証局テスト用サーバ証明書ポリシ：規程しない

１．３ 運営体制と証明書の適用範囲

１．３．１ 認証局の組織

(1) 意思決定組織

行政情報化推進会議において厚生労働省認証局の運営に関する意思決定を行う。

行政情報化推進会議において、厚生労働省認証局のＣＰ／ＣＰＳに関する決定及びその他厚生労働省認証局の運営に関する重要事項の決定を行う。

行政情報化推進会議は、厚生労働省認証局における以下の業務を厚生労働省認証局運営委員会に一任する。なお、厚生労働省認証局運営委員会の委員

長は、厚生労働省認証局責任者とし、大臣官房統計情報部企画課情報企画室長をもって充てるものとする。また、その他の委員は、委員長が指名する。

（厚生労働省認証局運営委員会の業務）

- 相互認証に関する決定
- 厚生労働省認証局の秘密鍵の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

(2) 厚生労働省認証局の組織

ブリッジ認証局への相互認証申請、厚生労働省における官職証明書発行申請受付及び審査並びに相互認証証明書、官職証明書、サーバ証明書の発行、更新、失効等の運営業務は、厚生労働省認証局責任者、発行局鍵管理者、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、厚生労働省認証局運用責任者、発行局操作員、登録局操作員、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。

１．３．２ 証明書の適用範囲

厚生労働省認証局に対して自己署名証明書を発行する。自己署名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10年とする。

ブリッジ認証局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年とする。

業務サーバ等に対してサーバ証明書を発行する。サーバ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年とする。

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、大臣官房統計情報部企画課情報企画室が行う。

１．４．２ 照会窓口

本ＣＰ／ＣＰＳに関する照会は、大臣官房統計情報部企画課情報企画室を窓口とする。

２．一般規定

２．１ 義務

２．１．１ 認証局業務に関する義務

厚生労働省認証局は、認証局業務に関して次の義務を負う。

- ブリッジ認証局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、サーバ証明書を発行する。
- 相互認証証明書の取り交わしに関しては、ブリッジ認証局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。
- 厚生労働省認証局の秘密鍵を安全に管理する。
- 厚生労働省認証局の秘密鍵が危殆化した場合は、速やかにブリッジ認証局運営組織に報告する。
- 厚生労働省認証局のシステムにおける発生事象を記録したログ（以下「監査ログ」という。）及びアーカイブデータを必要な期間保管する。
- 厚生労働省認証局のシステムの稼動監視を行う。

２．１．２ 登録局業務に関する義務

厚生労働省認証局は、登録局業務に関して次の義務を負う。

- 厚生労働省認証局は、ブリッジ認証局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ブリッジ認証局の公開鍵であり、かつブリッジ認証局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。
- 厚生労働省認証局が発行等する官職証明書、サーバ証明書の申請手続が適切に行われていることを確認する。

２．１．３ 証明書利用者の義務

厚生労働省認証局が発行する官職証明書の利用者は、次の義務を負う。

- 法令に基づき官職証明書を利用する場合は、本ＣＰ／ＣＰＳに従う。
- 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、厚生労働省電子署名規程等に基づいて行う。
- 官職の秘密鍵が危殆化した場合は、速やかに厚生労働省認証局責任者に報告する。

厚生労働省認証局が発行するサーバ証明書の利用者は、次の義務を負う。

・　法令に基づきサーバ証明書を利用する場合は、本ＣＰ／ＣＰＳに従う。
・　サーバ証明書及び業務サーバ等の秘密鍵を安全に管理する。
・　サーバ証明書の管理は、厚生労働省電子署名規程等に基づいて行う。
・　業務サーバ等の秘密鍵が危殆化した場合は、速やかに厚生労働省認証局責任者に報告する。

２．１．４　証明書検証者の義務

官職証明書及びサーバ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。

２．１．５　リポジトリに関する義務

厚生労働省認証局に関する情報のうち「２．６．１　厚生労働省認証局に関する情報の公表　（1）ブリッジ認証局の統合リポジトリ上での公表」は、ブリッジ認証局によって運用される統合リポジトリに複製する。

２．２　厚生労働省認証局の責任

厚生労働省認証局は、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、サーバ証明書の発行、更新、失効、保管及び公表に当たっては、ブリッジ認証局、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。

２．３　財務上の責任

規定しない。

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。

２．４．２　分割、存続、合併及び通知

規定しない。

２．４．３　紛争解決の手続

規定しない。

２．５ 料金

規定しない。

２．６ 公表とリポジトリ

２．６．１ 厚生労働省認証局に関する情報の公表

厚生労働省認証局に関する情報は、ブリッジ認証局の統合リポジトリ及び厚生労働省ホームページで公表する。

(1) ブリッジ認証局の統合リポジトリ上での公表

厚生労働省認証局は、厚生労働省認証局のリポジトリに保有する次の情報をブリッジ認証局の統合リポジトリに複製し、統合リポジトリ上で公表する。

- 厚生労働省認証局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、官職証明書及びそのＣＲＬ／ＡＲＬ
- 厚生労働省認証局が発行したサーバ証明書のうち、サーバの仕様上、証明書のリポジトリ上での公表が必要なもの

(2) 厚生労働省ホームページでの公表

厚生労働省認証局は、次の情報を厚生労働省ホームページで公表する。

- 厚生労働省認証局と相互認証した認証局の名称及び相互認証を取消した認証局の名称
- 厚生労働省認証局が認証した官職の名称及び認証を取消した官職の名称
- 厚生労働省認証局が認証した業務サーバ等の名称及び認証を取消した業務サーバ等の名称
- 厚生労働省認証局の秘密鍵の危殆化に関する情報
- 本ＣＰ／ＣＰＳ

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。

- 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、２．６．１(1)に該当するサーバ証明書及びそのＣＲＬ／ＡＲＬは、発行及び更新の都度
- 厚生労働省認証局と相互認証した認証局の名称及び相互認証を取消した認証局の名称は、厚生労働省認証局運営委員会による決定の都度
- 厚生労働省認証局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、厚生労働省認証局運営委員会による決定の都度
- 厚生労働省認証局が認証した業務サーバ等の名称及び認証を取消した業務サーバ等の名称は、厚生労働省認証局運営委員会による決定の都度

・　本ＣＰ／ＣＰＳの変更の都度

２．６．３ アクセス制御

厚生労働省認証局リポジトリから複製したブリッジ認証局の統合リポジトリ上で公表する情報及び厚生労働省ホームページで公表する情報は、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。

２．６．４ リポジトリ

厚生労働省認証局リポジトリに保有する情報のうち、「２．６．１ 厚生労働省認証局に関する情報の公表 (1) ブリッジ認証局の統合リポジトリ上での公表」において定める情報をブリッジ認証局の統合リポジトリに複製し公表する。

２．７ 準拠性監査

２．７．１ 監査頻度

厚生労働省認証局は監査人による監査を年１回定期的に実施する。また、厚生労働省認証局は、必要に応じて定期監査以外に監査を実施する。

２．７．２ 監査人の身元・資格

厚生労働省認証局の監査は、監査業務及び認証業務に精通した者が行う。

２．７．３ 監査人と被監査部門の関係

厚生労働省認証局の監査を実施する監査人は、厚生労働省認証局と利害関係を有しない者を選定する。

２．７．４ 監査内容

認証業務が本ＣＰ／ＣＰＳ、業務規定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。

２．７．５ 監査指摘事項への対応

厚生労働省認証局は、重要又は緊急を要する監査指摘事項について、厚生労働省認証局運営委員会の決定に基づき速やかに対応する。厚生労働省認証局の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、厚生労働省認証局の運用を停止するか否かは厚生労働省認証局運営委員会が決

定する。また、厚生労働省認証局運営委員会は、監査指摘事項に対して厚生労働省認証局が対策を実施したことを確認する。

２．７．６ 監査結果

厚生労働省認証局の監査結果は、監査人から厚生労働省認証局に対して監査報告書として提出される。厚生労働省認証局は、厚生労働省認証局運営委員会及びブリッジ認証局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。

２．８ 機密保持

２．８．１ 機密扱いとする情報

厚生労働省認証局は、漏えいすることによって厚生労働省認証局及びブリッジ認証局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。

２．８．２ 機密扱いとしない情報

厚生労働省認証局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。

２．８．３ 証明書失効情報の公表

厚生労働省認証局は、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、サーバ証明書の失効情報を公表する。

２．８．４ 法執行機関への情報開示

規定しない。

２．８．５ 民事手続上の情報開示

規定しない。

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。

２．８．７ その他の理由に基づく情報開示

規定しない。

２．９ 知的財産権

規定しない。

３．識別と認証

３．１ 初期登録

３．１．１ 名前の型

厚生労働省認証局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（以下ＤＮ（Distinguished Name）という。）の形式に従って設定する。

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。

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、ブリッジ認証局の定める規則に従う。

３．１．４ 名前の一意性

厚生労働省認証局の発行する証明書の主体者名は、一意に割り当てる。

３．１．５ 名前に関する紛争の解決手順

規定しない。

３．１．６ 商標の認識・認証・役割

規定しない。

３．１．７ 秘密鍵の所有を証明するための方法

(1) 相互認証手続き

厚生労働省認証局は、相互認証手続において、ブリッジ認証局から提出された証明書発行要求の署名の検証を行い、含まれているブリッジ認証局の公開鍵に対応するブリッジ認証局の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、ブリッジ認証局公開鍵の所有者を特定する。

(2) 官職証明書発行手続き

官職証明書発行手続において、以下のいずれかの方法により、公開鍵の所有者を特定する。

- 厚生労働省認証局で秘密鍵と公開鍵が対応する鍵ペアを生成する。
- 官職から提出された証明書発行要求の署名の検証を行い、含まれている官職の公開鍵に対応する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する。

(3) サーバ証明書発行手続き

サーバ証明書発行手続においては、以下のいずれかの方法により、業務サーバ等公開鍵の所有者を特定する。

- 厚生労働省認証局で秘密鍵と公開鍵が対応する鍵ペアを生成する。
- 業務サーバ等の管理責任者から提出された証明書発行要求の署名の検証を行い、含まれている業務サーバ等の公開鍵に対応する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する。

３．１．８ 組織の認証

厚生労働省認証局は、相互認証手続において、所定の手続に基づき、相互認証先の認証局を運営する者の真偽を確認する。

３．１．９ 個人の認証

厚生労働省認証局は、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。

３．２ 証明書の更新

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。

３．３ 証明書失効後の再発行

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。

３．４ 証明書の失効申請

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。

４．運用要件

４．１ 証明書の発行申請

(1) 自己署名証明書

厚生労働省認証局責任者が、発行局鍵管理者に対し発行指示を行う。

(2) 相互認証証明書

ブリッジ認証局に対する相互認証証明書の発行申請は、ブリッジ認証局の定める手続に基づいて行う。

(3) 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。

(4) サーバ証明書

サーバ証明書の発行申請は、所定の手続に基づいて行う。

４．２ 証明書の発行

(1) 自己署名証明書

厚生労働省認証局は、生成した認証局公開鍵に、厚生労働省認証局の署名を付して自己署名証明書を発行する。

(2) 相互認証証明書

厚生労働省認証局は、ブリッジ認証局の定める手続に基づく接続テスト完了後、ブリッジ認証局から提出された証明書発行要求に対し、厚生労働省認証局の署名を付して相互認証証明書を発行する。

(3) 官職証明書

以下のいずれかの方法により行うこととする。

- 厚生労働省認証局は、厚生労働省認証局で生成した公開鍵に、厚生労働省認証局の署名を付して官職証明書を発行する。
- 厚生労働省認証局は、官職から提出された証明書発行要求に対し、厚生労働省認証局の署名を付して官職証明書を発行する。

(4) サーバ証明書

以下のいずれかの方法により行うこととする。

- 厚生労働省認証局は、厚生労働省認証局で生成した公開鍵に、厚生労働省認証局の署名を付してサーバ証明書を発行する。

・　厚生労働省認証局は、業務サーバ等の管理責任者から提出された証明書発行要求に対し、厚生労働省認証局の署名を付してサーバ証明書を発行する。

(5)　テスト用証明書

厚生労働省認証局は、所定の方法で生成または他組織より受領した公開鍵に、厚生労働省テスト用認証局の署名を付与してテスト用証明書を発行する。

４．３ 証明書の受入れ

(1)　自己署名証明書

厚生労働省認証局は、発行した自己署名証明書を厚生労働省リポジトリ及び統合リポジトリに登録する。

(2)　相互認証証明書

厚生労働省認証局は、発行した相互認証証明書を、所定の手続に基づき、ブリッジ認証局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。

(3)　官職証明書

厚生労働省認証局は、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。

(4)　サーバ証明書

厚生労働省認証局は、発行したサーバ証明書を、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サーバ証明書の受入れの完了とする。

４．４ 証明書の失効と一時停止

４．４．１ 証明書の失効理由

(1)　自己署名証明書

厚生労働省認証局は、次の事由が発生した場合には、自己署名証明書を失効させる。

・　認証局秘密鍵の紛失及び危殆化

(2) 相互認証証明書

厚生労働省認証局は、厚生労働省認証局又はブリッジ認証局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。

- 厚生労働省認証局又はブリッジ認証局の秘密鍵の危殆化
- 相互認証基準違反
- 相互認証業務の終了
- 相互認証更新

(3) 官職証明書

厚生労働省認証局は、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
- 厚生労働省認証局の秘密鍵の紛失、危殆化
- 官職名等の変更、廃止

(4) サーバ証明書

厚生労働省認証局は、次のサーバ証明書失効事由が発生した場合、サーバ証明書を失効する。

- サーバ証明書の秘密鍵の紛失、危殆化
- 厚生労働省認証局の秘密鍵の紛失、危殆化
- サーバ名等の変更、廃止

４．４．２ 証明書の失効申請者

(1) 自己署名証明書

自己署名証明書の失効申請は、厚生労働省認証局責任者が行う。

(2) 相互認証証明書

ア ブリッジ認証局から相互認証証明書失効申請を受ける場合

ブリッジ認証局から厚生労働省認証局に対する失効申請は、ブリッジ認証局の責任者が行う。

イ ブリッジ認証局に相互認証証明書失効申請を行う場合

厚生労働省認証局からブリッジ認証局に対する失効申請は、厚生労働省認証局責任者が行う。

(3) 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。

(4) サーバ証明書

サーバ証明書の失効申請は、業務サーバ等の管理責任者が行う。

４．４．３ 証明書の失効申請及び失効処理手順

(1) 自己署名証明書

自己署名証明書を失効し、認証局失効リスト（以下「ＡＲＬ」という。）をブリッジ認証局の統合リポジトリに登録する。

(2) 相互認証証明書

ア ブリッジ認証局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。

イ ブリッジ認証局に相互認証証明書失効申請を行う場合

ブリッジ認証局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。

(3) 官職証明書

官職証明書の失効申請を受け取った厚生労働省認証局は、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、証明書失効リスト（以下「ＣＲＬ」という。）をブリッジ認証局の統合リポジトリに複製する。

(4) サーバ証明書

サーバ証明書の失効申請を受け取った厚生労働省認証局は、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、要求されたサーバ証明書を失効し、ＣＲＬをブリッジ認証局の統合リポジトリに複製する。

４．４．４ 失効における猶予期間

厚生労働省認証局は、失効申請手続の終了後、直ちに失効処理を行う。

４．４．５ 一時停止

厚生労働省認証局は、証明書の一時停止を行わない。

４．４．６ 一時停止申請者

規定しない。

４．４．７ 一時停止手順

規定しない。

４．４．８ 一時停止期間の制限

規定しない。

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、以下の状況においては、ＣＲＬ／ＡＲＬを直ちに発行する。

・証明書の失効を即座に周知する必要がある場合
・厚生労働省認証局の秘密鍵の危殆化等が発生した場合
・即座に発行する必要があると、厚生労働省認証局責任者が判断した場合

４．４．１０ ＣＲＬ／ＡＲＬの確認

証明書検証者は、厚生労働省認証局の発行する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。厚生労働省認証局は、この確認が行えるようブリッジ認証局の統合リポジトリ上でＣＲＬ／ＡＲＬを公表する。

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、ブリッジ認証局が維持管理する。

４．４．１２ オンライン有効性確認要件

規定しない。

４．４．１３ その他利用可能な有効性確認手段

規定しない。

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。

４．４．１５ 秘密鍵の危殆化に関する特別な要件

規定しない。

４．５ セキュリティ監査の手順

監査ログ検査者は、監査ログ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

厚生労働省認証局システム及び厚生労働省認証局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、操作ログ等の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）

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月次で行う。

４．５．３ 監査ログの保管期間

監査ログは３年間保管する。

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。

監査ログの退避（以下「バックアップ」という。）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。

なお、監査ログの閲覧及び削除は監査ログ検査者が行う。

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、月次で外部記憶媒体に取得する。

４．５．６ 監査ログの収集システム

監査ログの収集機能は厚生労働省認証局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。

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。

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。

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

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、３０年間保管する。

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。

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。

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。

４．６．６ アーカイブデータの収集システム

規定しない。

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。

４．７ 鍵更新

５年ごとに厚生労働省認証局の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厚生労働省認証局を廃止する場合は、こ

の限りでない。

厚生労働省認証局の鍵ペア更新時には、古い厚生労働省認証局の公開鍵と新しい厚生労働省認証局の公開鍵の認証パスを構築するリンク証明書を発行し、ブリッジ認証局の統合リポジトリ上で公表する。

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。

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、あらためて発行手続を行う。

４．８．３ 秘密鍵が危殆化した場合の対処

厚生労働省認証局の秘密鍵が危殆化した場合は、所定の手続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、サーバ証明書の失効手続
- 厚生労働省認証局の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、サーバ証明書の再発行手続

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。

４．８．４ 災害等発生時の設備の確保

災害等により厚生労働省認証局 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。

４．９ 認証業務の終了

行政情報化推進会議において厚生労働省認証局の認証業務の終了が決定した場合は、厚生労働省認証局運営委員会は、業務終了の事実、並びに業務終了後の厚生労働省認証局のシステム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。

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

厚生労働省認証局の施設は、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。

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厚生労働省認証局責任者が付与する。

厚生労働省認証局の施設は、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。

５．１．３ 電源設備と空調設備

厚生労働省認証局は、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。

５．１．４ 水害対策

厚生労働省認証局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。

５．１．５ 地震対策

厚生労働省認証局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。

５．１．６ 火災対策

厚生労働省認証局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。

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入出管理を行う。

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。

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厚生労働省認証局の施設と同等のセキュリティ対策を講ずる。

５．２ 手続面の管理

相互認証証明書、官職証明書、サーバ証明書の発行、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。

重要な業務の指示は、厚生労働省認証局責任者が厚生労働省認証局運用責任者に対して行い、厚生労働省認証局運用責任者は各操作員に対して作業指示書によって指示する。

操作員がシステム操作を行う際、厚生労働省認証局のシステムは、操作員が正当な権限者であることの識別・認証を行う。

各要員の業務を次のとおり定める。

⑴ 厚生労働省認証局責任者

厚生労働省認証局責任者は、厚生労働省認証局の運営に関する責任者であり、次の業務を行う。

- 厚生労働省認証局の運営方針の策定
- 認証業務の統括
- 厚生労働省認証局の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
- 厚生労働省認証局運用責任者等への作業指示及び作業結果の確認
- その他厚生労働省認証局の運営に関する統括

⑵ 発行局鍵管理者

発行局鍵管理者は、厚生労働省認証局の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、操作は複数人の発行局鍵管理者が行う。

・　セキュア暗号装置（以下「ＨＳＭ」という。）の機能を制御する鍵（以下「管理鍵」という。）の保管管理
・　厚生労働省認証局の秘密鍵のバックアップ媒体の保管管理
・　厚生労働省認証局の秘密鍵生成、自己署名証明書発行時のＨＳＭに対する鍵操作
・　厚生労働省認証局の秘密鍵の更新時におけるＨＳＭに対する鍵操作
・　厚生労働省認証局の秘密鍵のバックアップ、バックアップからの復元（以下「リストア」という）時のＨＳＭに対する鍵操作及び厚生労働省認証局の秘密鍵のバックアップ媒体のセット

(3)　受付担当者

受付担当者は、ブリッジ認証局からの相互認証証明書の発行要求の受付、官職証明書の発行申請の受付、サーバ証明書の発行申請の受付、申請者との連絡調整業務及び申請書類等の管理を行う。

(4)　審査担当者

審査担当者は、官職証明書、サーバ証明書の発行申請の審査業務を行う。

(5)　厚生労働省認証局運用責任者

厚生労働省認証局運用責任者は、厚生労働省認証局の運用に関する責任者であり、次の業務を行う。

・　相互認証証明書、官職証明書、サーバ証明書等の発行、更新、失効処理等の業務に関する発行局操作員、登録局操作員への作業指示および作業結果の確認
・　鍵の危殆化や災害発生などの緊急時における初期対応指示
・　認証局責任者への運用業務に関する作業結果の報告
・　その他厚生労働省認証局の運用に関する統括

(6)　発行局操作員

発行局操作員は、厚生労働省認証局の秘密鍵を使用する次の業務を行う。なお、操作は複数人の発行局操作員が行う。

・　厚生労働省認証局の秘密鍵を格納しているＨＳＭの活性化又は非活性化
・　厚生労働省認証局システムの起動又は停止
・　厚生労働省認証局システムの動作に関する設定変更管理
・　厚生労働省認証局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
- 証明書ポリシの設定登録又は変更
- 自己署名証明書、リンク証明書、相互認証証明書、サーバ証明書の発行、更新又は失効処理
- 操作員への証明書の発行、更新又は失効処理

(7) 登録局操作員

登録局操作員は、厚生労働省認証局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、操作は複数人の登録局操作員が行う。
- 官職証明書の発行、更新及び失効処理

(8) ディレクトリ操作員

ディレクトリ操作員は、厚生労働省認証局リポジトリの設定管理に関する業務を行う。

(9) 監査ログ検査者

監査ログ検査者は、厚生労働省認証局システム及び厚生労働省認証局リポジトリのログに関する次の業務を行う。
- 監査ログの検査
- 不要な監査ログの削除

５．３ 人事面の管理

厚生労働省認証局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、厚生労働省認証局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。

６．技術的セキュリティ管理

６．１ 鍵ペア生成とインストール

６．１．１ 鍵ペア生成

⑴ 厚生労働省認証局鍵

厚生労働省認証局の鍵ペアは、複数人の発行局鍵管理者がＦＩＰＳ１４０－１レベル３相当のＨＳＭを用いて生成する。

⑵ 官職証明書鍵

官職証明書の鍵ペアは、以下のいずれかの方法により生成する。

- 登録局操作員がソフトウェアを用いて生成する。
- 官職が、ＦＩＰＳ１４０－１レベル２相当以上のＨＳＭを用いて生成する。

⑶ サーバ証明書鍵

サーバ証明書の鍵ペアは、以下のいずれかの方法により生成する。

- 発行局操作員がソフトウェアを用いて生成する。
- 業務サーバ等の管理責任者が、所定の方法にて生成する。

６．１．２ 証明書利用者への秘密鍵配付

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。

サーバ証明書の秘密鍵は、「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。

６．１．３ 公開鍵の受領

⑴相互認証証明書の公開鍵

厚生労働省認証局は、相互認証証明書の取り交わしにおいて、ブリッジ認証局の公開鍵を安全かつ確実に受取る。

⑵官職証明書の公開鍵

厚生労働省認証局は、官職証明書の鍵ペア生成を官職者が行う場合、官職証明書の公開鍵を安全かつ確実に受取る。

⑶サーバ証明書の公開鍵

厚生労働省認証局は、サーバ証明書の鍵ペア生成を業務サーバ等の管理責任者が行う場合、官職証明書の公開鍵を安全かつ確実に受取る。

６．１．４ 厚生労働省認証局公開鍵の配付

厚生労働省認証局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。

６．１．５ 鍵のサイズ

(1) 厚生労働省認証局鍵

ＲＳＡ２０４８ビットの鍵を使用する。

(2) 官職証明書鍵

ＲＳＡ１０２４ビットの鍵を使用する。

(3) サーバ証明書鍵

ＲＳＡ５１２ビット以上の長さの鍵を使用する。

６．１．６ 公開鍵のパラメータの生成

規定しない。

６．１．７ 公開鍵パラメータの品質の検査

規定しない。

６．１．８ 鍵を生成するハードウェア／ソフトウェア

「６．１．１ 鍵ペア生成」において定める。

６．１．９ 鍵の利用目的

(1) 厚生労働省認証局鍵

厚生労働省認証局の秘密鍵は、署名に用いる。

(2) 官職証明書鍵

官職証明書の秘密鍵は、署名に用いる。

(3) サーバ証明書鍵

サーバ証明書の秘密鍵は、署名、データ暗号、鍵暗号の目的に用いる。

６．２ 秘密鍵の保護

６．２．１ 暗号モジュールに関する基準

(1) 厚生労働省認証局鍵

厚生労働省認証局の秘密鍵は、ＦＩＰＳ１４０－１レベル３相当のＨＳＭにより保護する。

(2) 官職証明書鍵

官職証明書の秘密鍵は、以下のいずれかの方法にて保護する。

- ＦＩＰＳ１４０－１レベル２相当以上のＩＣカード
- ＦＩＰＳ１４０－１レベル２相当以上のＨＳＭ

(3) サーバ証明書鍵

サーバ証明書の秘密鍵は、当該業務サーバ等の仕様に応じ、適切な保護機構を用い保護する。

６．２．２ 秘密鍵の複数人制御

厚生労働省認証局の秘密鍵を使用する操作は、複数人の発行局鍵管理者が行う。

６．２．３ 秘密鍵の預託

秘密鍵の預託は行わない。

６．２．４ 秘密鍵のバックアップ

厚生労働省認証局の秘密鍵のバックアップは、複数人の発行局鍵管理者が行う。

ＨＳＭからバックアップした厚生労働省認証局の秘密鍵は、暗号化して複数に分割し、複数人の発行局鍵管理者によって安全に保管する。

６．２．５ 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

６．２．６ 暗号モジュールへの秘密鍵の格納

(1) 厚生労働省認証局鍵

厚生労働省認証局の秘密鍵は、複数人の発行局鍵管理者が暗号モジュールの中で生成し、格納する。

(2)　官職証明書鍵

官職証明書の秘密鍵は、以下のいずれかの方法にて格納する。

・　登録局操作員が、暗号モジュールの中で生成し、格納する。
・　官職が、暗号モジュールの中で生成し、格納する。

(3)　サーバ証明書鍵

サーバ証明書の秘密鍵は、以下のいずれかの方法にて格納する。

・　発行局操作員が、暗号モジュールの中で生成し、格納する。
・　業務サーバ等の管理責任者が、暗号モジュールの中で生成し、格納する。

６．２．７ 秘密鍵の活性化方法

(1)　厚生労働省認証局鍵

厚生労働省認証局の秘密鍵は、複数人の発行局操作員により管理鍵を用いて活性化する。

(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 ）またはパスワードを用いて活性化する。

(3)　サーバ証明書鍵

サーバ証明書の秘密鍵は、業務サーバ等の管理責任者が適切な認証機構を用いて活性化する。

６．２．８ 秘密鍵の非活性化方法

(1)　厚生労働省認証局鍵

厚生労働省認証局の秘密鍵は、複数人の発行局操作員により管理鍵を用いて非活性化する。

(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またはパスワードを用いて非活性化する。

(3)　サーバ証明書鍵

サーバ証明書の秘密鍵は、業務サーバ等の管理責任者が、所定の手続きに従い非活性化する。

６．２．９ 秘密鍵の破棄方法

(1) 厚生労働省認証局鍵

ＨＳＭ内の厚生労働省認証局秘密鍵の破棄は、複数人の発行局鍵管理者が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、破棄する厚生労働省認証局の秘密鍵のバックアップ媒体を室外へ持ち出す場合も、物理的に媒体を破壊する。

(2) 官職証明書鍵

官職証明書の秘密鍵の破棄は、所定の手続に基づいて行う。

(3) サーバ証明書鍵

サーバ証明書の秘密鍵の破棄は、所定の手続に基づいて行う。

６．３ 公開鍵の履歴保管と鍵ペアの有効期間

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。

６．３．２ 公開鍵と秘密鍵の有効期間

(1) 厚生労働省認証局鍵

厚生労働省認証局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厚生労働省認証局を廃止する場合は、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。

(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。

(3) サーバ証明書鍵

サーバ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。

６．４ 活性化データ

６．４．１ 活性化データの生成とインストール

(1) 厚生労働省認証局鍵

厚生労働省認証局の秘密鍵を格納する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、発行局鍵管理者が決定しＨＳＭに直接入力する。

(2) 官職証明書鍵

官職証明書の秘密鍵を登録局操作員が生成し、ＩＣカードに格納する場合、初期ＰＩＮは、登録局操作員が設定する。

官職証明書の秘密鍵を官職が生成し、ＨＳＭに格納する場合、初期パスワードは、官職が設定する。

(3) サーバ証明書鍵

サーバ証明書の秘密鍵を発行局操作員が生成し、それを適切な保護機構により保護する場合、初期ＰＩＮまたはパスワードは、発行局操作員が設定する。

サーバ証明書の秘密鍵を業務サーバ等の管理責任者が生成し、ＨＳＭ又はＩＣカードに格納する場合、初期ＰＩＮまたはパスワードは、業務サーバ等の管理責任者が設定する。

６．４．２ 活性化データの保護

(1) 厚生労働省認証局鍵

厚生労働省認証局の秘密鍵を格納する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。

(2) 官職証明書鍵

官職証明書の秘密鍵を格納するＩＣカードまたはＨＳＭの活性化に必要なＰＩＮまたはパスワードは定期的に変更し、安全に保管する。

(3) サーバ証明書鍵

サーバ証明書の秘密鍵の活性化に、ＰＩＮ等が必要な場合は、ＰＩＮ等を定期的に変更し、安全に保管する。

６．５ コンピュータセキュリティ管理

６．５．１ コンピュータセキュリティ機能要件

厚生労働省認証局システムには、アクセス制御機能、操作員の識別と認証機能、監査ログ及びアーカイブデータの収集機能、厚生労働省認証局の鍵及びシステムのリカバリ機能等を備える。

６．５．２ コンピュータセキュリティ評価

規定しない。

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

６．６．１ システム開発面における管理

厚生労働省認証局のシステムの開発、修正又は変更に当たっては、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、厚生労働省認証局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。

６．６．２ システム運用面における管理

厚生労働省認証局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。

６．６．３ セキュリティ評価の基準

規定しない。

６．７ ネットワークセキュリティ管理

厚生労働省認証局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ブリッジ認証局の統合リポジトリに複製する。

６．８ 暗号モジュールの技術管理

「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。

７．証明書とＣＲＬ／ＡＲＬのプロファイル

７．１ 証明書のプロファイル

（１）自己署名証明書

項目	データ型	設定値	説明
Version	INTEGER	2	Version 3
SerialNumber	INTEGER		最大 32Byte
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
Issuer			証明書発行者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
OrganizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
OrganizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	Ministry of Health, Labour and Welfare	
OrganizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	MHLW Root CA	
Validity			証明書の有効期限
NotBefore	UTCTime		開始日時 *1 YYMMDDhhmmssZ 設定例：020328000000Z（証明書生成日）
NotAfter	UTCTime		終了日時 *1 YYMMDDhhmmssZ 設定例：120327235959Z（証明書生成日より 10 年）
Subject			証明書所有者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
OrganizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)

項目	データ型	設定値	説明
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
subjectPublicKeyInfo			証明書所有者の公開鍵情報
algorithm			
algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 1	rsaEncryption
parameters	NULL		
subjectPublicKey	BIT STRING		公開鍵値（鍵長2048bit）
Extensions			
KeyUsage			鍵の用途
extnID	OBJECT IDENTIFIER	2 5 29 15	
critical	BOOLEAN	TRUE	
extnValue	OCTET STRING		
KeyUsage	BIT STRING		keyCertSign(5) & cRLSign(6)
SubjectAltName			証明書所有者の代替名
extnID	OBJECT IDENTIFIER	2 5 29 17	
critical	BOOLEAN		
extnValue	OCTET STRING		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	日本国政府	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	厚生労働省	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	厚生労働省認証局	
BasicConstraints			基本制約
extnID	OBJECT IDENTIFIER	2 5 29 19	
critical	BOOLEAN	TRUE	
extnValue	OCTET STRING		
cA	BOOLEAN	TRUE	
CRLDistributionPoints			CRL 配布点
extnID	OBJECT IDENTIFIER	2 5 29 31	
critical	BOOLEAN		
extnValue	OCTET STRING		
[0]distributionPoint	DistributionPointName		
[0]fullName	GeneralNames		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
SubjectKeyIdentifier			証明書所有者の公開鍵の識別子

項目	データ型	設定値	説明
extnID	OBJECT IDENTIFIER	2 5 29 14	
critical	BOOLEAN		
extnValue	OCTET STRING		
SubjectKeyIdentifier			
KeyIdentifier	OCTET STRING		SubjectPublic Key の sha-1 ハッシュ値

*1:日時の指定は、すべてグリニッジ標準時で行う。

（２）相互認証証明書

項目	データ型	設定値	説明
Version	INTEGER	2	Version 3
SerialNumber	INTEGER		最大 32Byte
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
Issuer			証明書発行者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
OrganizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
OrganizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	Ministry of Health, Labour and Welfare	
OrganizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	MHLW Root CA	
Validity			証明書の有効期限
NotBefore	UTCTime		開始日時 *1 YYMMDDhhmmssZ 設定例：020401000000Z（証明書生成日）
NotAfter	UTCTime		終了日時 *1 YYMMDDhhmmssZ 設定例：070331235959Z（証明書生成日より 5 年）
Subject			証明書所有者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	

項目	データ型	設定値	説明
organizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	Bridge CA	
subjectPublicKeyInfo			証明書所有者の公開鍵情報
Algorithm			
algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 1	rsaEncryption
parameters	NULL		
subjectPublicKey	BIT STRING		公開鍵値（鍵長1024bit）
Extensions			
AuthorityKeyIdentifier			上位証明書の識別情報
extnID	OBJECT IDENTIFIER	2 5 29 35	
critical	BOOLEAN		
extnValue	OCTET STRING		
AuthorityKeyIdentifier			
[0]keyIdentifier	OCTET STRING		上位証明書の公開鍵の識別子
[1]authorityCertIssuer	GeneralName		上位証明書の情報
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
[2]authorityCertSerialNumber	INTEGER		上位証明書のシリアル番号
KeyUsage			鍵の用途
extnID	OBJECT IDENTIFIER	2 5 29 15	
critical	BOOLEAN	TRUE	
extnValue	OCTET STRING		
KeyUsage	BIT STRING		keyCertSign(5) & cRLSign(6)
BasicConstraints			基本制約
extnID	OBJECT IDENTIFIER	2 5 29 19	
critical	BOOLEAN	TRUE	
extnValue	OCTET STRING		
cA	BOOLEAN	TRUE	
CRLDistributionPoints			CRL 配布点
extnID	OBJECT IDENTIFIER	2 5 29 31	
critical	BOOLEAN		
extnValue	OCTET STRING		
[0]distributionPoint	DistributionPointName		

項目	データ型	設定値	説明
[0]fullName	GeneralNames		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
certificatePolicies			証明書ﾎﾟﾘｼｰ
extnID	OBJECT IDENTIFIER	2 5 29 32	
critical	BOOLEAN	TRUE	
extnValue	OCTET STRING		
policyIdentifier	OBJECT IDENTIFIER	1 2 392 100495 8 5 1 1 10	
policyQualifiers	PolicyQualifierInfo		
policyQualifierId	OBJECT IDENTIFIER	1 3 6 1 5 5 7 2 1	id-qt-cps
qualifier	IA5String	http://www.mhlw.go.jp/topics/bukyoku/toukei/cps/index.html	CPS 公開 URL)
PolicyMappings			証明書ﾎﾟﾘｼｰﾏｯﾋﾟﾝｸﾞ
extnID	OBJECT IDENTIFIER	2 5 29 33	
critical	BOOLEAN		
extnValue	OCTET STRING		
issuerDomainPolicy	OBJECT IDENTIFIER	1 2 392 100495 8 5 1 1 10	
subjectDomainPolicy	OBJECT IDENTIFIER	0 2 440 100145 8 1 1 1 10	id-bca-cp-ds.Class10
SubjectKeyIdentifier			証明書所有者の公開鍵の識別子
extnID	OBJECT IDENTIFIER	2 5 29 14	
critical	BOOLEAN		
extnValue	OCTET STRING		
SubjectKeyIdentifier			
KeyIdentifier	OCTET STRING		SubjectPublic Key の sha-1 ハッシュ値

*1:日時の指定は、すべてグリニッジ標準時で行う。

（３）リンク証明書

項目	データ型	設定値	説明
Version	INTEGER	2	Version 3
SerialNumber	INTEGER		最大 32Byte
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
issuer			証明書発行者の名称
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	

項目	データ型	設定値	説明
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
validity			証明書の有効期限
notBefore	UTCTime		開始日時 *1 YYMMDDhhmmssZ 設定例： OldWithNew： 020328000000Z (Old 生成日) NewWithOld： 0703DD000000Z (New 生成日)
notAfter	UTCTime		終了日時 *1 YYMMDDhhmmssZ 設定例： OldWithNew： 120327235959Z (Old 終了日) NewWithOld： 120327235959Z (Old 終了日)
subject			証明書所有者の名称
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
subjectPublicKeyInfo			証明書所有者の公開鍵情報
algorithm			
algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 1	rsaEncryption
parameters	NULL		

項目	データ型	設定値	説明
subjectPublicKey	BIT STRING		公開鍵値（鍵長2048bit）
Extensions			
AuthorityKeyIdentifier			上位証明書の識別情報
extnID	OBJECT IDENTIFIER	2 5 29 35	
critical	BOOLEAN		
extnValue	OCTET STRING		
AuthorityKeyIdentifier			
[0]keyIdentifier	OCTET STRING		上位証明書の公開鍵の識別子
[1]authorityCertIssuer	GeneralName		上位証明書の情報
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
[2]authorityCertSerialNumber	INTEGER		上位証明書のシリアル番号
KeyUsage			鍵の用途
ExtnID	OBJECT IDENTIFIER	2 5 29 15	
Critical	BOOLEAN	TRUE	
ExtnValue	OCTET STRING		
KeyUsage	BIT STRING		keyCertSign(5) & cRLSign(6)
SubjectAltName			証明書所有者の代替名
ExtnID	OBJECT IDENTIFIER	2 5 29 17	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	**日本国政府**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省認証局**	
IssuerAltName			証明書発行者の代替名
ExtnID	OBJECT IDENTIFIER	2 5 29 18	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		

項目	データ型	設定値	説明
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	**日本国政府**	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省**	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省認証局**	
BasicConstraints			基本制約
ExtnID	OBJECT IDENTIFIER	2 5 29 19	
Critical	BOOLEAN	TRUE	
ExtnValue	OCTET STRING		
CA	BOOLEAN	TRUE	
CRLDistributionPoints			CRL 配布点
ExtnID	OBJECT IDENTIFIER	2 5 29 31	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[0]distributionPoint	DistributionPointName		
[0]fullName	GeneralNames		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
CertificatePolicies			証明書ﾎﾟﾘｼｰ
ExtnID	OBJECT IDENTIFIER	2 5 29 32	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
policyIdentifier	OBJECT IDENTIFIER	2 5 29 32 0	ANY-POLICY
SubjectKeyIdentifier			証明書所有者の公開鍵の識別子
ExtnID	OBJECT IDENTIFIER	2 5 29 14	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
SubjectKeyIdentifier			
KeyIdentifier	OCTET STRING		SubjectPublic Key の sha-1 ハッシュ値

*1:日時の指定は、すべてグリニッジ標準時で行う。

（４）官職証明書

項目	データ型	設定値	説明
Version	INTEGER	2	Version 3
SerialNumber	INTEGER		最大 32Byte
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
Issuer			証明書発行者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
OrganizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
validity			証明書の有効期限
notBefore	UTCTime		開始日時 *1 YYMMDDhhmmssZ 設定例：020401000000Z（証明書生成日）
notAfter	UTCTime		終了日時 *1 YYMMDDhhmmssZ 設定例：050331235959Z（証明書生成日より３年）
subject			証明書所有者の名称
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記）必要に応じ階層化
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String		

項目	データ型	設定値	説明
commonName			一般名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 3	
value	UTF8String	Minister	**大臣の例**
subjectPublicKeyInfo			証明書所有者の公開鍵情報
algorithm			
algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 1	rsaEncryption
parameters	NULL		
subjectPublicKey	BIT STRING		公開鍵値（鍵長1024bit
Extensions			
AuthorityKeyIdentifier			上位証明書の識別情報
extnID	OBJECT IDENTIFIER	2 5 29 35	
critical	BOOLEAN		
extnValue	OCTET STRING		
AuthorityKeyIdentifier			
[0]keyIdentifier	OCTET STRING		上位証明書の公開鍵の識別子
[1]authorityCertIssuer	GeneralName		上位証明書の情報
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
[2]authorityCertSerialNumber	INTEGER		上位証明書のシリアル番号
KeyUsage			鍵の用途
ExtnID	OBJECT IDENTIFIER	2 5 29 15	
Critical	BOOLEAN	TRUE	
ExtnValue	OCTET STRING		
KeyUsage	BIT STRING		digitalSignature (0) & nonRepudiation (1)
SubjectAltName			証明書所有者の代替名
ExtnID	OBJECT IDENTIFIER	2 5 29 17	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	**日本国政府**	

項目	データ型	設定値	説明
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省**	
organizationalUnitName			組織内ユニット名 必要に応じ階層化
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String		
commonName			**一般名**
type	OBJECT IDENTIFIER	2 5 4 3	
value	UTF8String	**大臣**	**大臣の例**
IssuerAltName			証明書発行者の代替名
ExtnID	OBJECT IDENTIFIER	2 5 29 18	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	**日本国政府**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省認証局**	
CRLDistributionPoints			CRL 配布点
ExtnID	OBJECT IDENTIFIER	2 5 29 31	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[0]distributionPoint	DistributionPointName		
[0]fullName	GeneralNames		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
certificatePolicies			証明書ポリシー
ExtnID	OBJECT IDENTIFIER	2 5 29 32	
Critical	BOOLEAN	TRUE	
ExtnValue	OCTET STRING		
policyIdentifier	OBJECT IDENTIFIER	1 2 392 100495 8 5 1 1 10	
policyQualifiers	PolicyQualifierInfo		
policyQualifierId	OBJECT IDENTIFIER	1 3 6 1 5 5 7 2 1	id-qt-cps
qualifier	IA5String	http://www.mhlw.go.jp/topics/bukyoku/toukei/cps/index.html	CPS 公開 URL
SubjectKeyIdentifier			証明書所有者の公開鍵の識別子
ExtnID	OBJECT IDENTIFIER	2 5 29 14	

項目	データ型	設定値	説明
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
SubjectKeyIdentifier			
KeyIdentifier	OCTET STRING		SubjectPublic Key の sha-1 ハッシュ値

*1:日時の指定は、すべてグリニッジ標準時で行う。

（５）サーバ証明書

項目	データ型	設定値	説明
Version	INTEGER	2	Version 3
SerialNumber	INTEGER		最大 32Byte
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
Issuer			証明書発行者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
OrganizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
validity			証明書の有効期限
notBefore	UTCTime		開始日時 *1 YYMMDDhhmmssZ 設定例：020401000000Z（証明書生成日）
notAfter	UTCTime		終了日時 *1 YYMMDDhhmmssZ 設定例：050331235959Z（証明書生成日より３年）
subject			証明書所有者の名称
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)

項目	データ型	設定値	説明
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名（英語表記）必要に応じ階層化
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
X.520 id-at 以下に定義される任意の属性、または emailAddress			サーバ名等（英語表記）
type	OBJECT IDENTIFIER	先頭が"2 5 4"で始まる任意の OBJECT IDENTIFIER または、" 1 2 840 113549 1 9 1"	
value	TeletexString PrintableString UniversalString IA5String UTF8String のいずれか		
subjectPublicKeyInfo			証明書所有者の公開鍵情報
algorithm			
algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 1	rsaEncryption
parameters	NULL		
subjectPublicKey	BIT STRING		公開鍵値（鍵長 1024bit 以上）
Extensions *2			
AuthorityKeyIdentifier	OBJECT IDENTIFIER	2 5 29 35	上位証明書の識別情報
KeyUsage	OBJECT IDENTIFIER	2 5 29 15	鍵の用途
SubjectAltName	OBJECT IDENTIFIER	2 5 29 17	証明書所有者の代替名
IssuerAltName	OBJECT IDENTIFIER	2 5 29 18	証明書発行者の代替名
CRLDistributionPoints	OBJECT IDENTIFIER	2 5 29 31	CRL 配布点
certificatePolicies	OBJECT IDENTIFIER	2 5 29 32	証明書ﾎﾟﾘｼｰ
SubjectKeyIdentifier	OBJECT IDENTIFIER	2 5 29 14	証明書所有者の公開鍵の識別子
extKeyUsage	OBJECT IDENTIFIER	2 5 29 37	拡張鍵使用目的
authorityInfoAccess	OBJECT IDENTIFIER	1 3 6 1 5 5 7 1 1	発行者情報アクセス

*1:日時の指定は、すべてグリニッジ標準時で行う。
*2:業務サーバの使用目的によっては、以下の項目の一部又は全部を付加しない場合がある。また、付加する場合、その拡張領域の値は、業務サーバの使用目的・仕様によって個々に定める。

（6）テスト用証明書

規定しない。

７．２ ＣＲＬ／ＡＲＬのプロファイル

項目	データ型	設定値	説明
Version	INTEGER	1	Version 2
Signature			証明書への署名に使用される署名ｱﾙｺﾞﾘｽﾞﾑ
Algorithm	OBJECT IDENTIFIER	1 2 840 113549 1 1 5	Sha-1WithRSAEncryption
Parameters	NULL		
Issuer			証明書発行者の名称
CountryName			国名
Type	OBJECT IDENTIFIER	2 5 4 6	
Value	PrintableString	JP	
organizationName			組織名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 10	
Value	UTF8String	Japanese Government	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ﾕﾆｯﾄ名(英語表記)
Type	OBJECT IDENTIFIER	2 5 4 11	
Value	UTF8String	MHLW Root CA	
ThisUpdate	UTCTime		今回更新日時 *1 YYMMDDhhmmssZ 設定例：更新時刻の GMT 変換値
NextUpdate	UTCTime		次回更新日時 *1 YYMMDDhhmmssZ 設定例：更新日+48 時間の GMT 変換値 2 日間(48 時間)有効
revokedCertificates			失効証明書ﾘｽﾄ(SEQUENCE)
userCertificate	INTEGER		失効証明書 serialNumber
revocationDate	UTCTime		証明書失効日時 *1 YYMMDDhhmmssZ
crlEntryExtensions			組織内ﾕﾆｯﾄ名(英語表記)
reasonCode			証明書失効理由(必要に応じて設定)
ExtnID	OBJECT IDENTIFIER	2 5 29 21	
Critical	BOOLEAN		
extnValue	OCTET STRING		

項目	データ型	設定値	説明
CRLReason	ENUMERATED		以下の何れかを設定する 1：鍵危殆(keyCompromise) 2：CA 鍵危殆(cACompromise) 3：所属変更(affiliationChanged) 4：上書(superseded) 5：業務停止(cessationOfOperation)
invalidityDate			証明書失効事象発生日時(必要に応じて設定)
ExtnID	OBJECT IDENTIFIER	2 5 29 24	
Critical	BOOLEAN		
extnValue	OCTET STRING		
invalidityDate	GeneralizedTime		失効事象発生日時 *1 YYYYMMDDhhmmssZ
CrlExtensions			
AuthorityKeyIdentifier			上位証明書の識別情報
ExtnID	OBJECT IDENTIFIER	2 5 29 35	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
AuthorityKeyIdentifier			
[0]keyIdentifier	OCTET STRING		上位証明書の公開鍵の識別子
[1]authorityCertIssuer	GeneralName		上位証明書の情報
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名(英語表記)
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
[2]authorityCertSerialNumber	INTEGER		上位証明書のシリアル番号
IssuerAltName			証明書発行者の代替名
ExtnID	OBJECT IDENTIFIER	2 5 29 18	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
[4]directoryName	Name		

項目	データ型	設定値	説明
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	**日本国政府**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省**	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	**厚生労働省認証局**	
CRLNumber			CRL 番号
ExtnID	OBJECT IDENTIFIER	2 5 29 20	
Critical	BOOLEAN		
ExtnValue	OCTET STRING		
cRLNumber	INTEGER		最大 32Byte
issuingDistributionPoint			発行する配布点
ExtnID	OBJECT IDENTIFIER	2 5 29 28	
Critical	BOOLEAN	TRUE	
ExtnValue	OCTET STRING		
[0]distributionPoint	DistributionPointName		
[0]fullName	GeneralNames		
[4]directoryName	Name		
countryName			国名
type	OBJECT IDENTIFIER	2 5 4 6	
value	PrintableString	JP	
organizationName			組織名
type	OBJECT IDENTIFIER	2 5 4 10	
value	UTF8String	Japanese Government	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	Ministry of Health, Labour and Welfare	
organizationalUnitName			組織内ユニット名
type	OBJECT IDENTIFIER	2 5 4 11	
value	UTF8String	MHLW Root CA	
[1] onlyContainsUserCerts	BOOLEAN	TRUE	**CRL の場合**
[2] onlyContainsCACerts	BOOLEAN	TRUE	**ARL の場合**

*1:日時の指定は、すべてグリニッジ標準時で指定する。

８．ＣＰ／ＣＰＳの管理

８．１　ＣＰ／ＣＰＳの変更

行政情報化推進会議は、本ＣＰ／ＣＰＳを必要に応じて変更する。

８．２　ＣＰ／ＣＰＳの公表と通知

厚生労働省認証局運営委員会は、本ＣＰ／ＣＰＳが変更された場合、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。

８．３　ＣＰ／ＣＰＳ　の決定

厚生労働省認証局のＣＰ／ＣＰＳは、行政情報化推進会議の了承をもって有効なものとする。