オンライン請求ネットワーク関連システム
共通認証局運用規程
(Certification Practice Statement)

令和８年４月

社会保険診療報酬支払基金

国 民 健 康 保 険 中 央 会

改訂履歴

日付	改訂事由
令和元年/12/27	・初版
令和２年/6/12	・1.3　PKI の関係者 　加入者へ市町村国保を追加 ・1.3.1　認証局 　本認証局運営委員会の更新 ・オンライン請求システム・オンライン資格確認等システム向けの電子証明書発行に伴う更新
令和２年/9/24	・1.3　PKI の関係者 　加入者の追加 　サービス提供者の追加 ・1.4.2　証明書の有効期間 　システムベンダ・販売会社の証明書有効期間の追加 ・1.4.3　証明書の用途 　サーバ証明書を利用できるシステム及びサービス提供者の説明を追加 ・9.1　料金 　オン請求・オン資格用証明書の発行（更新）の費用追加
令和４年/9/22	・1．2　文書名と識別 　タイムスタンプ証明書ポリシーへの言及を追記 ・1．4．1　証明書の種類 　「（５）タイムスタンプ証明書 」の説明を追記 ・1．4．2　証明書の有効期間 　「（５）タイムスタンプ証明書 」の説明を追記 ・1．4．3　証明書の用途 　タイムスタンプの用途に関する説明を追記 ・1．5．2　問合せ先 　「社会保険診療報酬支払基金」の「窓口」の部署名を更新 ・1．6　用語の定義 　No.54 「タイムスタンプ証明書」を追加

	・6．3．2　公開鍵証明書の有効期間及び鍵ペアの使用期間 「(５)タイムスタンプ証明書 」の説明を追記 ・6．4．2　活性化データの保護 タイムスタンプ証明書への言及を追記 ・7．1　証明書のプロファイル 「7．1．10　拡張キー」を追加 「表 10．タイムスタンプ証明書（オン請求・オン資格システム)」を追加 ・9．18　附則 適用開始日を追記
令和 5 年/3/17	・1.3　PKI の関係者 加入者へ自治体、福祉事務所を追加 ・7．1　証明書のプロファイル 「表８．サーバ証明書（医療保険者等向け中間サーバ等システム)」に Subject Alternative Name（サブジェクト代替名（SAN)）の領域を追加
令和 5 年/10/1	9.1.1　証明書の発行又は更新料 郵送手数料を更新
令和 5 年/11/22	・1．3 PKI の関係者 「図１．関係者」にデジタル庁国民向けサービスグループを追加 ・1．4．3　証明書の用途 「表１．サーバ証明書を利用できるシステム及びサービス提供者」に 8 PMH デジタル庁国民向けサービスグループを追加 ・1.6　用語の定義 「表２．用語」に Public Medical Hub について追加
令和 5 年/12/19	・1．3　PKI の関係者 「図１．関係者 証明書発行対象者・検証者 オン請求・オン資格システムの加入者」に、訪問看護ステーションを追加 ・1．3．2　証明書発行対象者・検証者 「(4) [オン請求・オン資格システム]加入者」に、訪問看護ステーションを追加 ・3．1．2　識別名に関する要件

	「表４．識別名に関する命名規則（オン請求・オン資格システム)」に、訪問看護に関する記載事項を追加
令和 6 年/4/16	・1．3 PKI の関係者 「図１．関係者 証明書発行対象者・検証者 オン請求・オン資格システムの加入者」に、職域診療所を追加 ・1．3．2 証明書発行対象者・検証者 「(4) [オン請求・オン資格システム]加入者」に、職域診療所を追加 ・1．5．2 問合せ先 「国民健康保険中央会」の「窓口」の部署名を更新 ・3．1．2 識別名に関する要件 「表４．識別名に関する命名規則（オン請求・オン資格システム)」に、訪問看護に関する記載事項を追加
令和 6 年/10/1	・9．1．1 証明書の発行又は更新料 郵送手数料の改訂 ・9．6．2 加入者の責務 「(3) 秘密鍵等の管理責任」に、バックアップに関する表記を追記 ・9．6．4 サービス提供者の責務 「(3) 秘密鍵等の管理責任」に、バックアップに関する表記を追記 ・9．18 附則 適用開始日を追記
令和 7 年/2/19	・1．3 PKI の関係者 「図１．関係者 証明書発行対象者・検証者 オン請求・オン資格システム 加入者」に、消防庁/消防本部を追加 ・1．3．2 証明書発行対象者・検証者 「(4) [オン請求・オン資格システム]加入者」に、消防庁/消防本部を追加 ・3．1．2 識別名に関する要件 「表４．識別名に関する命名規則（オン請求・オン資格システム)」に、消防本部に関する記載事項を追加

	・3．2．2 証明書発行対象者・検証者の審査 消防庁/消防本部に関する記載を追加 ・4．9．2 失効の依頼者 消防庁/消防本部に関する記載を追加 ・6．1．2 証明書発行対象者への秘密鍵の送付 消防庁/消防本部に関する記載を追加 ・9．1．1　証明書の発行又は更新料 消防庁/消防本部に関する記載を追加 ・9．18　附則 適用開始日を追記
令和 7 年/8/7	・1．4．3 証明書の用途 「表１．サーバ証明書を利用できるシステム及びサービス提供者」に電子処方箋管理サービス、電子カルテ情報共有サービス、予診情報・予防接種記録管理／請求支払システムを追加 ・1．5．2 問合せ先 「社会保険診療報酬支払基金」の「窓口」の部署名を更新 ・4．3．2 認証局発行の通知 消防庁/消防本部に関する記載を追加
令和 8 年 4/1	・9．1．1　証明書の発行又は更新料 郵送手数料の改訂

目　　次

1　概説

本章は、本認証局の概要、関係者、証明書の用途及び用語の定義等について記述する。

1．1　概要

この証明書ポリシー／認証局運用規程（以下、「本 CP/CPS」という。）は、証明書の適切な運用・管理に関する諸手続を定めることを目的とする。本 CP/CPS は、本認証局が認証業務を行う際の運用に関する規程であり、発行局及び登録局を含む本認証局の運用方針、加入者・サービス提供者と本認証局との関係、本認証局が加入者・サービス提供者に対して発行する証明書の取り扱い等を定めている。加入者・サービス提供者証明書の取り扱いには、申請・登録・発行・更新・再発行・失効・有効期間満了に関する記述、及び発行方針と利用に関連する要件が含まれる。

本 CP/CPS は、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」のフレームワークに準拠している。

本 CP/CPS は、本認証局が発行する電子証明書のプロファイルについても定める。本認証局は、証明書毎の証明書ポリシー（以下、「CP」という。）を個別に定めず、本 CP/CPS が CP を包含するものとする。

1．2　文書名と識別

本 CP/CPS の正式名称は、「オンライン請求ネットワーク関連システム共通認証局運用規程（Certification Practice Statement)」とする。

なお、中間サーバについては、本認証局の利用者証明書ポリシー、サーバ証明書ポリシー、コード署名証明書ポリシー及びタイムスタンプ証明書ポリシーを含む本 CP/CPS の識別子は、次のとおりとする。

0.2.440.200317.1.1.1　（社会保険診療報酬支払基金）

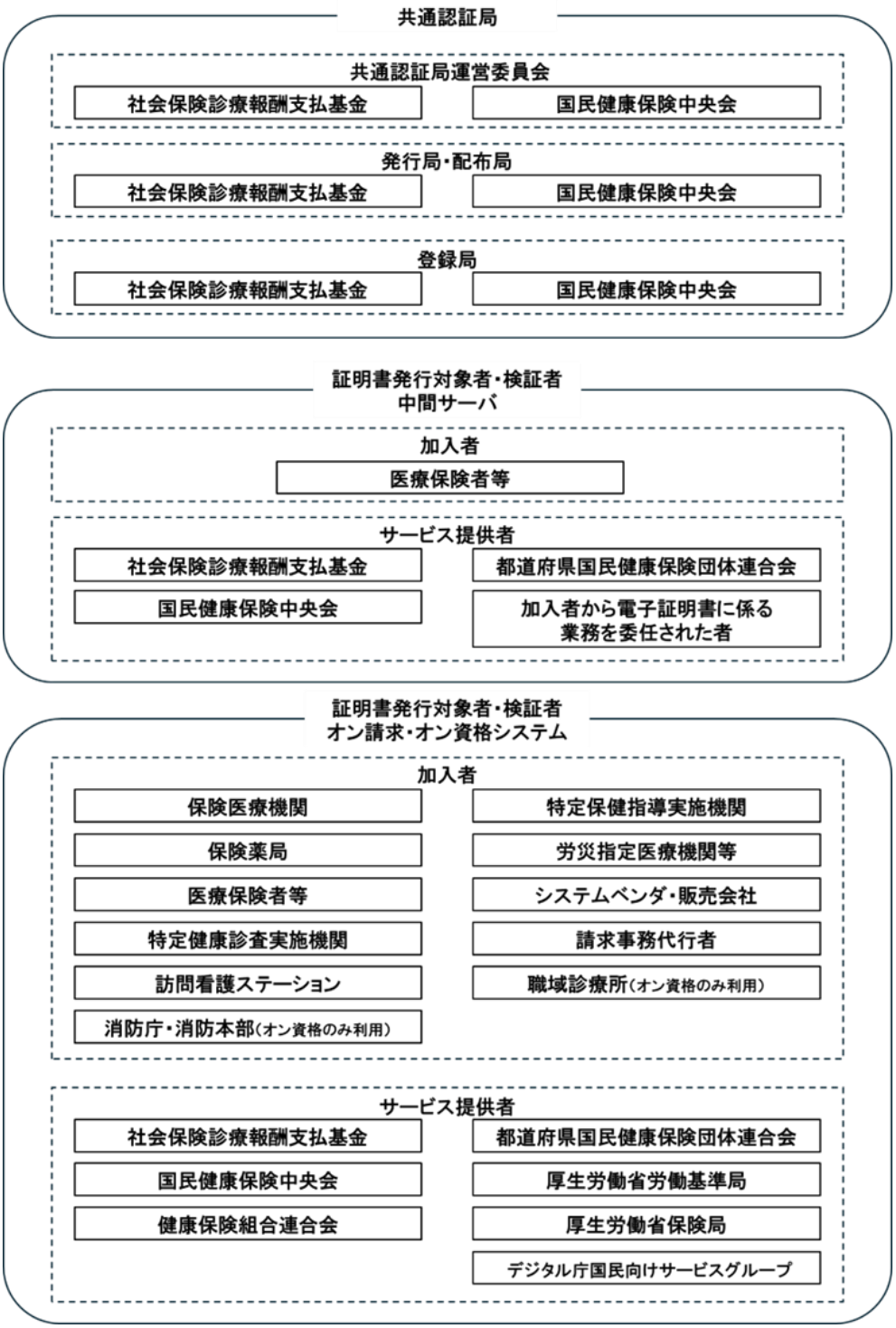
0.2.440.200318.1.1.1　（国民健康保険中央会）

1．3　PKI の関係者

本認証局は、医療保険者等向け中間サーバ（以下、「中間サーバ」という。）とオンライン請求（以下、「オン請求」という）・オンライン資格確認（以下、「オン資格」という。）用の証明書で証明書発行対象者・検証者が異なる。

関係者を「図 1. 関係者」に示す。各関係者は、本 CP/CPS が定める義務を遵守するものとする。

図１．関係者


共通認証局
共通認証局運営委員会
社会保険診療報酬支払基金
国民健康保険中央会
発行局・配布局
社会保険診療報酬支払基金
国民健康保険中央会
登録局
社会保険診療報酬支払基金
国民健康保険中央会
証明書発行対象者・検証者
中間サーバ
加入者
医療保険者等
サービス提供者
社会保険診療報酬支払基金
都道府県国民健康保険団体連合会
国民健康保険中央会
加入者から電子証明書に係る
業務を委任された者
証明書発行対象者・検証者
オン請求・オン資格システム
加入者
保険医療機関
特定保健指導実施機関
保険薬局
労災指定医療機関等
医療保険者等
システムベンダ・販売会社
特定健康診査実施機関
請求事務代行者
訪問看護ステーション
職域診療所（オン資格のみ利用）
消防庁・消防本部（オン資格のみ利用）
サービス提供者
社会保険診療報酬支払基金
都道府県国民健康保険団体連合会
国民健康保険中央会
厚生労働省労働基準局
健康保険組合連合会
厚生労働省保険局
デジタル庁国民向けサービスグループ

1．3．1　認証局

本認証局は、運営方針を協議する本認証局運営委員会、登録局、発行局及び配布局より構成される。

（１）本認証局運営委員会

ア　構成

① 認証局運営委員会は、認証局運営委員により構成する。

② 認証局運営委員は、別途定める認証局運営委員会規程に基づき、社会保険診療報酬支払基金及び国民健康保険中央会から選出する。

イ　役割

① 認証局責任者、認証局副責任者、それぞれ１名を選任する。

② 認証局の運営方針に関する事項について協議する。

③ CP/CPSの策定、管理及び改定に関する事項について協議する。

④ 認証局運用体制の策定に関する事項について協議する。

⑤ 協議事項について、認証局運営委員会で承認の上、社会保険診療報酬支払基金及び国民健康保険中央会に報告する。

ウ　協議事項

① 認証局責任者、認証局副責任者に関する事項

② 認証局の運営方針に関する事項

③ 認証局運用規程の策定、管理及び改定に関する事項

④ 認証局運用体制の策定に関する事項

⑤ 認証局の秘密鍵危殆化時の対応に関する事項

⑥ 災害発生等による緊急時の対応に関する事項

⑦ 電子証明書発行（更新）費用に関する事項

⑧ 認証局の関係経費に関する事項

⑨ その他認証局の運営に関する事項

⑩ 認証局を構築及び運営する上での方針となる文書と本CP/CPSの適合性判断に関する事項

（２）登録局

登録局は、証明書発行対象者からの依頼に対して、依頼内容の適切な審査及び登録業務を行い、発行局への証明書の発行要求及び失効要求を行う。

登録局は、社会保険診療報酬支払基金及び国民健康保険中央会がその役割を担う。

（３）発行局

発行局は、登録局からの証明書の発行要求及び失効要求に基づき証明書の発行及び失効の処理を行う。

発行局は、社会保険診療報酬支払基金及び国民健康保険中央会がその役割を担う。

（４）配布局

配布局は、発行局で発行した証明書の失効情報等の提供を行う。
また、加入者・サービス提供者への証明書の配付を行う。
配布局は、社会保険診療報酬支払基金及び国民健康保険中央会がその役割を担う。

1．3．2　証明書発行対象者・検証者

本認証局の証明書発行は、中間サーバ、オン請求・オン資格システムそれぞれの「1.3 関係者」で示す証明書発行対象者・検証者に対し行う。

（１）[中間サーバ]加入者

中間サーバを利用する加入者とは、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）に基づき、個人番号利用事務実施者として中間サーバを利用する者を指す。加入者の範囲は以下のとおりとする。

ア　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第二に基づき、健康保険法（大正11 年法律第70 号）による保険給付の支給、保健事業若しくは福祉事業の実施又は保険料等の徴収に関する事務を行う全国健康保険協会

イ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第四に基づき、船員保険法（昭和14 年法律第73 号）による保険給付、障害前払一時金若しくは遺族前払一時金の支給、保健事業若しくは福祉事業の実施若しくは保険料等の徴収又は雇用保険法等の一部を改正する法律（平成19 年法律第30 号）附則第39 条の規定によりなお従前の例によるものとされた平成19 年法律第30 号第4 条の規定による改正前の船員保険法による保険給付の支給に関する事務を行う全国健康保険協会

ウ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第二に基づき、健康保険法による保険給付の支給、保健事業若しくは福祉事業の実施又は保険料等の徴収に関する事務を行う健康保険組合

エ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第三十に基づき、国民健康保険法（昭和33 年法律第192 号）による保険給付の支給、保険料の徴収又は保健事業の実施に関する事務を行う国民健康保険組合

オ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第五十九に基づき、高齢者の

医療の確保に関する法律（昭和57 年法律第80 号）による後期高齢者医療給付の支給、保険料の徴収又は保健事業の実施に関する事務を行う後期高齢者医療広域連合

カ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第二十八に基づき、国家公務員共済組合法（昭和33 年法律第128 号）による短期給付の支給又は福祉事業の実施に関する事務を行う国家公務員共済組合

キ　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第三十九に基づき、地方公務員等共済組合法（昭和37 年法律第152 号）による短期給付若しくは年金である給付の支給若しくは福祉事業の実施又は地方公務員等共済組合法の長期給付等に関する施行法（昭和37 年法律第153 号）による年金である給付の支給に関する事務を行う地方公務員共済組合

ク　行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25 年法律第27 号）別表第一第二十二に基づき、私立学校教職員共済法（昭和28 年法律第245 号）による短期給付若しくは年金である給付の支給又は福祉事業の実施に関する事務を行う日本私立学校振興・共済事業団

ケ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）（利用範囲）第九条に基づき、健康保険法（大正十一年法律第七十号）第四十八条若しくは第百九十七条第一項による別表第一の上欄に掲げる行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者又は地方公共団体の長その他の執行機関による第一項又は前項に規定する事務の処理に関して必要とされる他人の個人番号を記載した書面の提出その他の他人の個人番号を利用した事務を行う市町村

コ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）別表第一第十五に基づき、生活保護法（昭和25年法律第144号）による保護の決定及び実施、就労自立給付金若しくは進学準備給付金の支給、被保護者健康管理支援事業の実施、保護に要する費用の返還又は徴収金の徴収に関する事務を行う都道府県知事、市長（特別区の区長を含む。）又は社会福祉法（昭和26年法律第45号）に規定する福祉に関する事務所を管理する町村長

（２）[中間サーバ]サービス提供者

サービス提供者とは、中間サーバに関連するサービスを提供する者を指す。

具体的には、社会保険診療報酬支払基金、国民健康保険中央会、都道

府県国民健康保険団体連合会及び加入者から電子証明書に係る業務を委任された者等（ASP 事業者等）のその他適当と認められる者とする。

（３）[中間サーバ]検証者

検証者とは、証明書を検証する者を指す。加入者とサービス提供者の間で証明書を用いた認証を行う場合、サービス提供者の証明書の検証者は加入者となり、加入者の証明書の検証者はサービス提供者となる。

（４）[オン請求・オン資格システム]加入者

加入者とは、オン請求・オン資格システムを利用する者を指す。加入者の範囲は以下のとおり。

ア　健康保険法第六十三条第三項第一号の規定による保険医療機関及び保険薬局

イ　国民健康保険法第三十六条第三項の規定による保険医療機関及び保険薬局

ウ　社会保険診療報酬支払基金法第一条及び第十五条に基づき契約する保険者等

エ　高齢者の医療の確保に関する法律第二十八条の規定による健康保険法第六十三条第三項各号に掲げる病院又は診療所その他適当と認められるもの（特定健康診査実施機関、特定保健指導実施機関）

オ　労働者災害補償保険法施行規則第十一条 第一項の規定による 労働者災害補償保険法第二十九条第一項の 社会復帰促進等事業として設置された 病院若しくは診療所又は都道府県労働局長の指定する病院若しくは診療所、薬局（労災指定医療 機関 等）

カ　商業登記簿の写しで確認可能なレセプトコンピュータやオンライン資格確認端末等のシステム開発及びシステム販売を行う会社（システムベンダ・販売会社）

キ　療養の給付及び公費負担医療に関する費用の請求に関する省令第四条の規定による請求事務代行者（医師会等）

ク　健康保険法第八十八条第一項に基づき訪問看護事業を実施する指定訪問看護事業者の訪問看護ステーション

ケ　健康保険法第六十三条第三項第二号及び第三号の規定による職域診療所

コ　消防組織法第二条の規定による消防庁

サ　消防組織法第九条第一号の規定による消防本部

（５）[オン請求・オン資格システム]サービス提供者

サービス提供者とは、オンライン請求関連ネットワーク内に設置のシステムに関連するサービスを提供する者を指す。

（６）[オン請求・オン資格システム]検証者

検証者とは、証明書を検証する者を指す。加入者とサービス提供者の間で証明書を用いた認証を行う場合、サービス提供者の証明書の検証者は加入者となり、加入者の証明書の検証者はサービス提供者となる。

（７）その他の関係者

本認証局にその他の関係者は存在しない。

1．4　証明書の用途

本節は、本認証局で発行する証明書の用途について記述する。

1．4．1　証明書の種類

本認証局は、以下の証明書を発行する。詳細は、「7.1.9 証明書ポリシーの拡張フィールド」に示す。

（１）認証局自己署名証明書

認証局自己署名証明書は、本認証局自身の電子証明書であり、本認証局の公開鍵に対して本認証局の署名鍵で電子署名されている。本認証局の署名鍵は、加入者・サービス提供者に配付される証明書及び CRL への電子署名の用途に使用される。

（２）利用者証明書

加入者・サービス提供者向けに発行される電子証明書である。本認証局は、本認証局の判断及び管理の下、動作確認を目的とした証明書の発行・失効を行うことができるものとする。

（３）サーバ証明書

サービス提供者向けに発行される電子証明書である。サーバ認証に利用される。本認証局は、本認証局の判断及び管理の下、本認証局運営委員会から許可を得たオンライン請求関連ネットワーク内に設置のシステムに対し、証明書の発行・失効を行うことができるものとする。

（４）コード署名証明書

サービス提供者向けに発行される電子証明書である。配布するアプリケーションへ電子署名するために利用される。本認証局は、本認証局の判断及び管理の下､証明書の発行･失効を行うことができるものとする。

（５）タイムスタンプ証明書

サービス提供者向けに発行される電子証明書である。タイムスタンプへ電子署名するために利用される。本認証局は、本認証局の判断及び管理の下、証明書の発行・失効を行うことができるものとする。

1．4．2　証明書の有効期間

本認証局が発行する電子証明書の有効期間は、以下のとおりとする。

（１）認証局自己署名証明書：13 年 3 ヶ月

（２）利用者証明書：3 年 3 ヶ月
　　システムベンダ・販売会社のみ：1 年
（３）サーバ証明書：3 年 3 ヶ月
（４）コード署名証明書：3 年 3 ヶ月
（５）タイムスタンプ証明書：10 年

1．4．3　証明書の用途

本認証局で発行する証明書及び対応する鍵ペアは、以下の用途で使用できる。
なお、詳細は「4.5 証明書の利用」に記述する。
（１）システムを利用する際の認証及び暗号化通信。
（２）サービス提供者が提供するアプリケーションに対する電子署名及び検証。
（３）本認証局で発行するサーバ証明書を利用できるシステム及びサービス提供者は「表 1. サーバ証明書を利用できるシステム及びサービス提供者」に示す。
（４）サービス提供者が生成する対象データへのタイムスタンプに対する電子署名及び検証。

表１．サーバ証明書を利用できるシステム及びサービス提供者

No	システム名	サービス提供者
1	医療保険等向け中間サーバー等システム	社会保険診療報酬支払基金 国民健康保険中央会
2	オンライン請求システム	社会保険診療報酬支払基金 国民健康保険中央会 都道府県国民健康保険団体連合会
3	オンライン資格確認等システム	社会保険診療報酬支払基金 国民健康保険中央会
4	特定健診等データ収集システム 特定健診等データ管理システム	社会保険診療報酬支払基金 都道府県国民健康保険団体連合会 国民健康保険中央会
5	高額医療交付金オンライン申請システム	健康保険組合連合会
6	労災レセプト電算処理システム	厚生労働省労働基準局
7	保険医療機関等管理システム	厚生労働省保険局
8	Public Medical Hub	デジタル庁国民向けサービスグループ
9	電子処方箋管理サービス	社会保険診療報酬支払基金 国民健康保険中央会
10	電子カルテ情報共有サービス	社会保険診療報酬支払基金

		国民健康保険中央会
11	予診情報・予防接種記録管理／請求支払システム	国民健康保険中央会

1．5　認証局運用規程の管理

本節は、本 CP/CPS の管理を行う者の組織、電話番号等の連絡先について記述する。

なお、本 CP/CPS の改定手続きについては「9.12 改定」で記述する。

1．5．1　管理組織

本 CP/CPS の管理組織は、社会保険診療報酬支払基金及び国民健康保険中央会で構成する本認証局運営委員会とする。

1．5．2　問合せ先

本 CP/CPS に関する問合せ先は以下のとおりとする。

社会保険診療報酬支払基金
窓口：社会保険診療報酬支払基金　情報基盤部
受付時間：平日9:00～17:00
電話番号：03-3591-7501

国民健康保険中央会
窓口：国民健康保険中央会　保健福祉部医療保険情報提供等実施機関担当室
受付時間：平日9:00～17:00
電話番号：03-6268-8890

1．5．3　適合性の判断者

本認証局を構築及び運営する上での方針となる文書と本CP/CPSの適合性についての判断は、本認証局運営委員会が行う。

1．5．4　承認手続

本 CP/CPS は、本認証局運営委員会において協議及び承認の上、社会保険診療報酬支払基金及び国民健康保険中央会に報告する。

1．6　用語の定義

本 CP/CPS で使用する用語の意味を「表２．用語」に示す。

表２．用語

No.	用語	意味
1	CP （Certificate Policy）	特定のコミュニティ、かつ／又は、共通のセキュリティ要件をもつアプリケーションのクラスへの証明書の適用可能性を示すルールの命名された集合。
2	CPS （Certification Practice Statement）	証明書ポリシーに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。
3	CRL （Certificate Revocation List）	有効期限内の証明書を失効した際に記載される証明書の失効リスト（証明書失効リス）。失効リストには証明書を特定する証明書シリアル番号や失効理由等の情報が記載される。
4	DN （Distinguished Name）	識別名を意味し、組織名やユーザ名等をカンマで区切って並べたもの。証明書では「 c=JP 、 o= ○○…」の記法にて証明書の所有者を識別する。
5	FIPS 140-2 レベル 3 （Federal Information Processing Standard）	米国連邦政府にてハードウェア及びソフトウェアの暗号モジュールに対するセキュリティ要件を規定したもの。
6	HSM （Hardware Security Modules）	暗号処理機能を有し、認証局秘密鍵をハードウェア内部で安全に管理する装置（鍵管理装置）。認証局 秘密 鍵は HSM 内部にて生成され、 HSM の外部へ鍵を取り出すことは出来ない。鍵の使用も活性化データと PIN （パスワード）により鍵への不正アクセスを防止している。
7	IETF RFC3647 （Internet Engineering Task Force Request For Comment）	認証局運用規程の記載項目について、IETF （インターネットで利用される技術について標準化する組織）によって標準化された規約のこと。
8	Issuer	証明書の発行者を意味し、本認証局が Issuer に該当する。

No.	用語	意味
9	ITU-T X.500（International Telecommunication Union -Telecommunication sector）	ITU-T は国際電気通信連合の電気通信標準部門であり、通信分野の標準を策定している。 X.500 は ITU T にて定められたディレクトリサービスの規格のこと。
10	ITU-T X.509	ITU-T にて定められた電子証明書及び証明書失効リストの標準仕様のこと。
11	OCSP（Online Certificate Status Protocol）	証明書の有効性を検証するプロトコル。証明書の有効性を検証したい検証者は、OCSP サーバに検証依頼を行うことにより、リアルタイムに失効有無の確認が可能となる。
12	OID（Object ID）	オブジェクト識別子を参照のこと。
13	RSA Encryption（Rivest Shamir Adleman）	RSA 公開鍵暗号のことで、暗号／復号及び電子署名を行う。
14	SHA1（Secure Hash Algorithm 1）	ハッシュ関数の一つ。 任意の長さのデータから 160 ビットのハッシュ値を生成するハッシュ関数のこと。
15	SHA256（Secure Hash Algorithm 256）	ハッシュ関数の一つ。任意の長さのデータから 256 ビットのハッシュ値を生成するハッシュ関数のこと。SHA1 の後継規格である SHA2 の一部として定義されている。
16	SSL（Secure Socket Layer）	Netscape 社が開発した通信の暗号化や通信相手を識別する技術のこと。
17	Subject	主体者（証明書の所有者）を表す識別名のこと。
18	TLS（Transport Layer Security）	IETF によって標準化された通信の暗号化や通信相手を識別する技術のこと。
19	暗号モジュール	暗号機能を備えたハードウェア又はソフトウェアのこと。
20	一意性	１つに特定できる性質を意味する。
21	依頼書	利用者証明書の発行依頼及び失効依頼を行う際の依頼文書のこと。

No.	用語	意味
22	エントリ	情報の名簿（一覧）のこと。
23	オブジェクト識別子	組織や文書等を電子的に識別するために、全世界で一意になるように割り当てられた番号のこと。
24	鍵ペア	公開鍵暗号で生成される一組の鍵のこと。一組の鍵とは、秘密鍵と公開鍵を指す。
25	活性化	ハードウェア又はソフトウェアに備えられた機能により、機器を使用できる状態にすること。
26	活性化データ	活性化を行うためのデータのこと。
27	監査ログ	システムの操作及び証明書発行／失効等の処理を行った際に記載されるログ（証跡情報）のうち、監査に使用されるログのこと。
28	危殆化	データの信頼性を失うこと。鍵の危殆化とは、本人のみが保管している秘密鍵の情報が漏洩等により、信頼性を失うことを指す。
29	キャビネット	戸棚のこと。資料及び電子媒体等を保管するのに利用される。
30	公開鍵	公開鍵暗号方式にて生成される鍵ペアのうち、本人以外にも公開する鍵のこと。公開鍵は証明書内に記載される。
31	公開鍵アルゴリズム	暗号をする鍵と復号をする鍵が異なる暗号演算方式（公開鍵暗号方式）のことであり、それぞれの鍵のことを秘密鍵、公開鍵と呼ぶ。
32	コード署名証明書	配布するアプリケーションへ電子署名するために利用する証明書のこと。アプリケーションに付与された電子署名により、アプリケーションの提供者の正当性を検証することができる。
33	サーバ証明書	SSL を行うときに必要となるサーバの証明書のこと。サーバ認証に利用される。
34	自己署名証明書	認証局自身の証明書のこと。

No.	用語	意味
35	主体者公開鍵情報アルゴリズム	証明書の主体者(証明書の所有者)が持つ公開鍵のアルゴリズム（手順）のこと。
36	証明書ステータス	証明書の状態を指す。証明書の状態には有効（利用可能状態)、失効（利用不可状態）があり、証明書の有効期限や CRL から状態を確認する。
37	署名アルゴリズム	証明書上の署名(Signature)の項目に記載される、署名用アルゴリズム（手順）のこと。
38	脆弱性	コンピュータやネットワークなどの情報システムにおいて、システムに権限のない者が悪意に利用できてしまう欠陥や仕様上の問題等のこと。
39	相互運用	複数の認証局が相互接続する場合に、相手側の認証局が発行した証明書を、信頼を保ちつつ相互に利用できるようにするための運用のこと。
40	タイムスタンプ	ファイル等に記録された日時情報のこと。ある処理がいつ実施されたかを記載するために用いられる。
41	バックアップデータ	保存されたデータのこと。バックアップデータはハードウェアの故障等の際にシステムを復元するために利用される。
42	ハッシュ関数	任意の長さのデータから固定長の疑似乱数を生成する演算手法のこと。
43	ハッシュ値	ハッシュ関数により生成した値のこと。
44	パラメータ	ソフトウェアが処理を行う際に与える設定情報であり、この情報によりソフトウェアの処理内容又は処理結果が変化する。
45	非活性化	ハードウェア又はソフトウェアに備えられた機能により、機器を使用できない状態にすること。
46	秘密鍵	公開鍵暗号方式にて生成される鍵ペアのうち、所有者本人のみが保有する鍵のこと。

No.	用語	意味
47	秘密鍵の預託	秘密鍵を第三者へ預けること。第三者へ秘密鍵を預けることにより、秘密鍵の厳重な管理及び消失時の復元を可能とする。
48	ファイアウォール	部外者が無断でネットワークやコンピュータへ侵入出来ないように防御するシステムのこと。
49	プロファイル	証明書及び CRL に記載された情報。証明書の有効期間や識別名等もプロファイルの情報である。
50	証明書ポリシー	共通のセキュリティ要件を満たした規程を意味する名称のこと。他の規程と区別する際に使用される。
51	証明書のライフサイクル	証明書の生成から廃棄までの一連の流れ。
52	リポジトリ	証明書の検証が行えるように CRL 等の情報が格納されている保管場所のこと。
53	利用者証明書	加入者・サービス提供者が使用する証明書のこと。
54	タイムスタンプ証明書	タイムスタンプへ電子署名するために利用する証明書のこと。タイムスタンプに付与された電子署名により、対象データがタイムスタンプ付与時点で存在していたことを証明することができる。
55	Public Medical Hub	マイナンバーカードを「公費負担」・「地方単独医療費助成の受給者証」、「予防接種の接種券」及び「母子保健の受診券」として利用できるようにするため、自治体と医療機関との間でこれらに関する情報を連携する機能を持つシステム

2　公開とリポジトリ

本章は、本認証局で公開する情報とリポジトリについて記述する。

2．1　リポジトリ

リポジトリとは、検証を行う際に必要となる証明書の失効情報等が格納されている保管場所のことをいう。リポジトリの公開は、24 時間 365 日利用可能とする。ただし、リポジトリのメンテナンス等が生じる場合には、この限りでないものとする。

2．2　公開情報

本認証局は、証明書の失効情報及び本 CP/CPS を関係者に対して公開する。

2．3　公開の頻度

本 CP/CPS は、内容が改定された時点で速やかに公開する。
CRL については、発行した CRL の有効期間を 7 日間とし、「4.9.7 CRL 発行頻度」による周期で更新する。

2．4　リポジトリへのアクセス管理

本認証局は、リポジトリに対する情報セキュリティ対策以外の目的で特段のアクセス管理は行わない。

3　識別及び認証

本章は、証明書の識別及び認証について記述する。

3．1　名称

本章は、証明書の識別名並びに証明書の発行、 更新及び失効時の認証について記述する。

3．1．1　識別名の形式

証明書の識別名の形式は、ITU-T X.500 の識別名（DN）の規定に従う。

3．1．2　識別名に関する要件

証明書の識別名は、認証等を行う検証者に理解される必要がある。本認証局は、「表３．　識別名に関する命名規則（中間サーバ）　」及び「表４．識別名に関する命名規則（オン請求・オン資格システム)」のとおり記載する。

表３．識別名に関する命名規則（中間サーバ）

証明書対象	項目	記載内容
本表共通	国（Country）	日本国（JP）を記載する。
	組織名（Organization）	中間サーバに係る認証局（Intermediate Server）を記載する。
医療保険者等	組織単位名（Organizational Unit）	組織の種別として、医療保険者（insurance）を記載する。
	一般名（Common Name）	保険者コード（8 桁固定）を記載する。
サービス提供者	組織単位名（Organizational Unit）	サービスの種別として、 サーバ証明書（Server）、 社会保険診療報酬支払基金及び国民健康保険中央会が利用する証明書及び加入者から電子証明書に係る業務を委任された者が管理する機器が利用する証明書（insurance）を記載する。
	一般名（Common Name）	サーバ証明書の場合、ドメイン名を記載する。 保守用証明書の場合、その用途が理解できる名称を記載する。

証明書対象	項目	記載内容
証明書発行者 （認証局）	一般名 （Common Name）	証明書発行者の名称として、オンライン請求ネットワーク関連システム共通認証局（Online Billing NW Common Root CA -G*）を記載する。 -*は認証局秘密鍵の世代を記載する。

表４．識別名に関する命名規則（オン請求・オン資格システム）

証明書対象	項目	記載内容
本表共通	国（Country）	日本国（JP）を記載する。
	組織名 （Organization）	オンライン請求システム （ReceiptOnline）を記載する。
保険医療機関 保険薬局 労災指定医療機関等 請求事務代行者 訪問看護ステーション	組織単位名 （Organizational Unit）	所在する都道府県名をヘボン式のローマ字で記載する。
	組織単位名 （Organizational Unit）	組織の種別として、 医科（medical）、歯科（dental）、調剤（pharmacy）又は訪問看護（nursing）を記載する。
	一般名 （Common Name）	一般名についても一意に識別可能とするため、都道府県番号（2 桁）、点数表番号（1 桁）及び医療機関コード又は薬局コード（7 桁）を連結した 10 桁固定のコード又は事務代行者コード 10 桁固定を記載する。
医療保険者	組織単位名 （Organizational Unit）	組織の種別として、医療保険者 （insurance）を記載する。
	一般名 （Common Name）	保険者番号（8 桁固定）を記載する。
特定健康診査実施機関 特定保健指導実施機関	組織単位名 （Organizational Unit）	所在する都道府県名をヘボン式のローマ字で記載する。
	組織単位名 （Organizational Unit）	組織の種別として、健診（kenshin）を記載する。

証明書対象	項目	記載内容
	一般名 （Common Name）	一般名についても一意に識別可能とするため、特定健診・特定保健指導機関コード（10 桁）を記載する。
職域診療所 ※	組織単位名 （Organizational Unit）	所在する都道府県名をヘボン式のローマ字で記載する。
	組織単位名 （Organizational Unit）	職域診療所（shokuiki）を記載する。
	一般名 （Common Name）	一般名についても一意に識別可能とするため、都道府県番号（2 桁）、点数表番号（1 桁）及び職域診療所コード（7 桁）を連結した 10 桁固定のコードを記載する。
システムベンダ・販売会社	組織単位名 （Organizational Unit）	組織の種別として、メーカ（maker）を記載する。
	一般名 （Common Name）	システムベンダ・販売会社に対して発行したシステムベンダ・販売会社コード（10　桁）を記載する。
サービス提供者	組織単位名 （Organizational Unit）	サービスの種別として、サーバ証明書（Server）又は保守用証明書（support）を記載する。
	一般名 （Common Name）	サーバ証明書の場合、ドメイン名を記載する。 保守用証明書の場合、その用途が理解できる名称を記載する。
証明書発行者 （認証局）	一般名 （Common Name）	証明書発行者の名称として、オンライン請求ネットワーク関連システム 共通認証局（Online Billing NW Common Root CA -G*）を記載する。 -*は認証局秘密鍵の世代を記載する。

証明書対象	項目	記載内容
消防本部 ※	組織単位名 （Organizational Unit）	所在する都道府県名をヘボン式のローマ字で記載する。
	組織単位名 （Organizational Unit）	組織の種別として、消防本部 （shoubou） を記載する。
	一般名 （Common Name）	一般名についても一意に識別可能とするため、都道府県番号（2 桁）、点数表番号（1 桁）及び消防本部コード(7 桁)を連結した 10 桁固定のコードを記載する。

※ オン資格システムのみ利用

3．1．3　匿名又は仮名

匿名又は仮名による識別名の記載は許可しない。

本認証局で発行する証明書に記載する識別名は、「表２．　識別名に関する命名規則（中間サーバ)」「表３．識別名に関する命名規則（オン請求・オン資格システム)」のとおり記載する。

3．1．4　識別名を解釈するための規則

識別名を解釈するための規則は、ITU-T X.500 識別名（DN）及び識別名に関する要件に従う。

3．1．5　識別名の一意性

証明書の識別名は、証明書発行対象者を一意に識別可能としない。ただし、証明書のシリアル番号により、証明書発行対象者を一意に識別することができる。

3．1．6　商標

本認証局は、証明書の識別名に商標が含まれているかの確認は行わない。

3．2　新規の証明書発行の本人性確認

本節は、新規に証明書を発行する際の認証について記述する。

3．2．1　秘密鍵の所持を確認する方法

本認証局は、加入者・サービス提供者に配付される秘密鍵を生成し、「6.1.2 証明書発行対象者への秘密鍵の送付」の定めに従い配付を行う。同配付をもって、加入者・サービス提供者が秘密鍵を保有したものとみなす。

3．2．2　証明書発行対象者・検証者の審査

加入者及びサービス提供者から証明書の発行依頼を受領した場合は、依頼を行った証明書発行対象者・検証者が適切かを社会保険診療報酬支払基金及び国民健康保険中央会が所有する情報と依頼情報との検証により審査を行う。

審査の結果、加入者あてに発行通知書等の送付を行うが、社会保険診療報酬支払基金及び国民健康保険中央会が所有する住所へ書留・簡易書留等で郵送することにより本人性の確認を担保するものとする。

ただし、加入者が消防本部の場合、消防庁が加入者の本人性の確認を行い、証明書の発行は社会保険診療報酬支払基金及び国民健康保険中央会が実施するものとする。

社会保険診療報酬支払基金及び国民健康保険中央会は、消防庁からの証明書の発行申請の受領をもって、本人性の確認の審査が実施されたものとする。

また、サービス提供者のうち、都道府県国民健康保険団体連合会から証明書の発行依頼を受領した場合は、加入者と交わした委任状の写し等と依頼書との検証により審査を行う。加入者から電子証明書に係る業務を委任された者等のその他適当と認められる者から証明書の発行依頼を受領した場合は、これに加え登記事項証明書等の公的文書により審査を行う。

なお、医療保険者等の廃止等に伴う移管先の保険者より証明書の申請を行えることとする。この場合、社会保険診療報酬支払基金及び国民健康保険中央会が所有する移管元と移管先を記す情報と依頼情報との検証により審査を行う。

3．2．3　個人の審査

本認証局は、個人に対しての証明書の発行は行わないため、個人の審査は行わない。

3．2．4　確認しない情報

依頼に記載されている項目のうち、証明書に記載する情報はすべて確認を行う。

3．2．5　権限の確認

本認証局の審査により、証明書発行対象者・検証者証明書の発行依頼を行う権限を保持しているかの確認を行う。

3．2．6　他の認証局との相互運用の基準

本認証局は、他の認証局との相互運用は行わない。

3．3　証明書更新時の本人性確認

本節は、証明書を更新する際の本人性について記述する。

3．3．1　加入者の場合

本認証局は、SSL クライアント認証を伴う証明書更新申請において、申請者から提示された利用者証明書が、本認証局から発行された証明書であることをもっ

て更新時の本人性確認とする。それ以外の証明書更新申請については、「3.2 新規の証明書発行時の本人性確認」に規定された方法に従う。

3．3．2　サービス提供者の場合

新規発行時と同様の取扱いとする。具体的には、「3.2 新規の証明書発行時の本人性確認」に規定された方法に従う。

3．4　証明書失効時の本人性確認

本認証局は、発行申請時に本認証局から通知された本認証局と加入者・サービス提供者のみが知る情報の提示を受け、照合を行う。又は、新規発行時と同様の取扱いとし、「3.2 新規の証明書発行時の本人性確認」に規定された方法と同様とする。

4　証明書のライフサイクル

本章は、証明書のライフサイクルである発行、更新及び失効における手続き等について記述する。

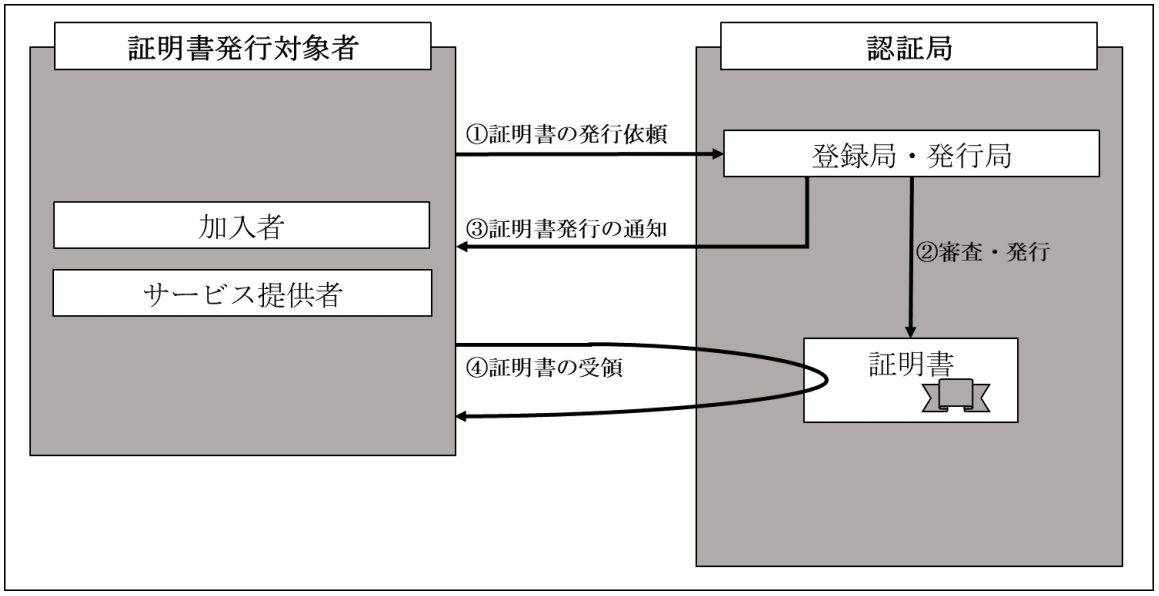
4．1　申請の手続

本節は、証明書の発行の依頼を行う者及びその手続きについて記述する。

4．1．1　証明書の発行依頼

新規に証明書を発行する際の流れを「図２．新規の証明書発行の流れ」に示す。

図２．新規の証明書発行の流れ



4．1．2　証明書発行の依頼者

証明書発行対象者のみが、本認証局に対して証明書の発行を依頼できる。なお、電子証明書の発行は、端末ごとに依頼する。

4．2　審査の手続

本節は、発行依頼を受領した際の審査の手続きについて記述する。

4．2．1　本人性及び資格の確認

本人性及び資格の確認については「3.2 新規の証明書発行時の本人性確認」に記述する。

4．2．2　発行依頼の承認

本人性等の確認及びその他発行依頼に関わる内容の確認を行った後、発行依頼を承認する。ただし、発行依頼に関わる内容の記載不備又は社会保険診療報酬支払基金及び国民健康保険中央会の所有する情報と不整合が存在する場合等、審査過程において疑義が生じた場合は、証明書の発行依頼を却下する。その場合は、依頼者に通知する。

4．2．3　審査にかかる期間

本認証局の登録局が「4.2 審査」の基準に基づき申請を処理した後、発行局は速やかに証明書を発行する。

4．3　発行の手続

本節は、証明書の発行を行う際の手続きについて記述する。

4．3．1　証明書の発行

証明書の発行を行う際には、本認証局で秘密鍵及び公開鍵の鍵ペアを生成し証明書を発行する。発行した証明書及び秘密鍵は暗号化し、保管する。

4．3．2　認証局発行の通知

本認証局は、証明書の発行に関して以下のいずれかの通知を加入者・サービス提供者に行う。

（１）証明書を取得するために必要な情報を、配達状況を確認できる方法（書留や簡易書留）で送付する。
（２）証明書を格納した電子媒体を手交する。
（３）加入者が消防本部の場合、消防庁が加入者のメールアドレスの真正性の確認を実施していることから、当該メールアドレスに証明書を取得するために必要な情報を送付する。

4．4　受領の手続

本節は、証明書が受領された際の手続きについて記述する。

4．4．1　証明書の受領

（１）加入者については、証明書及び秘密鍵の取得を行った証跡をもって依頼者が証明書を受領したこととみなす。一定の期間内に証明書が受領されない場合は、証明書を失効する。
（２）医療保険者等向け中間サーバ等に関連するサービス提供者については、受領書の提出をもって依頼者が証明書を受領したこととみなす。一定の期間内に受領書が提出されない場合は、証明書を失効する。
（３）「4　証明書のライフサイクル」に示す依頼した端末ごとに電子証明書をインストールする。

4．4．2　証明書の公開

本認証局は、各証明書発行対象者の証明書の公開は行わない。

4．4．3　その他の関係者への通知

本認証局にその他の関係者は存在しないため、通知しない。

4．5　証明書の利用

本節は、証明書を受領した後の鍵ペアと証明書の利用に関する責任について記述する。証明書の利用は、自身の証明書及び秘密鍵を利用する場合と他者の証明書を検証する場合に分けて記述する。

4．5．1　自身の証明書の利用

自身の証明書及び秘密鍵を利用する際は、「7.1 証明書のプロファイル」に定める鍵用途（Key Usage）に限ることとする。また、証明書の利用にあたっては、「9.6 関係者の責務」の内容を遵守すること。

4．5．2　他者の証明書の利用

他者の証明書を検証に利用する際は、「7.1 証明書のプロファイル」に定める鍵用途（Key Usage）に限ることとする。

また、証明書の検証にあたっては、「9.6.3 検証者の責務」の内容を遵守すること。

4．6　鍵更新を伴わない更新の手続

本認証局は、基本的に鍵更新を伴わない証明書の更新は行わない。

4．7　鍵更新を伴う更新の手続

本節は、鍵更新を伴う証明書の更新を行う際の手続きについて記述する。

4．7．1　証明書更新の要件

本認証局は、以下の条件に該当する場合を除き証明書の更新を行う。

（１）更新実施時に証明書が失効している場合。

（２）更新実施時に証明書の記載内容に変更がある場合。

4．7．2　更新の依頼者

証明書の更新の依頼者は、「1.3.2 証明書発行対象者・検証者」に示す証明書発行対象者・検証者とする。

4．7．3　更新の手続

証明書の有効期限が90日未満となっている証明書に対し、証明書の更新を行う。更新時の証明書の発行は、証明書の更新アプリケーション又は更新サイトによる申請、あるいは「4.3.1 証明書の発行」に示す新規の証明書発行時と同様の

手順で行う。

4．7．4　更新された証明書の発行通知

本認証局は、証明書の更新アプリケーション又は更新サイトによる申請においては画面表示など明示的に通知を行い、書留や簡易書留による通知は行わない。

4．7．5　更新された証明書の受領

更新された証明書の受領は、証明書の更新アプリケーション又は更新サイトにより依頼者が当該証明書の取得をもって証明書を受領したこととみなす。

4．7．6　更新された証明書の公開

本認証局は、各証明書発行対象者の証明書の公開は行わない。

4．7．7　その他の関係者への通知

本認証局にその他の関係者は存在しないため、通知しない。

4．8　証明書の変更

本認証局は､発行した証明書の変更は行わない｡証明書の変更が必要な場合は、失効手続きを行った後に、再度、新規に発行を行うものとする。

4．9　失効の手続き

本節は、証明書の失効を行う際の手続きについて記述する。

4．9．1　証明書失効の要件

証明書の失効は、証明書発行対象者からの依頼による場合と本認証局の判断による場合がある。

（１）証明書発行対象者の依頼による失効

証明書発行対象者は、下記の事項に該当する場合は、直ちに本認証局に対し、証明書の失効を依頼しなければならない。

・秘密鍵が危殆化し、機密性が失われた場合又はその可能性がある場合
・証明書の記載事項が事実と異なる場合
・証明書が不要となった場合
・その他、証明書発行対象者が失効を必要と判断する場合

（２）本認証局の判断による失効

本認証局は、下記の事項に該当する事由の発生を認識し、証明書の有効性が損なわれると判断した場合には、本認証局の判断により証明書発行対象者の属する加入者・サービス提供者が所有するすべての証明書の失効を行う。

・証明書発行対象者が本CP/CPSに基づく義務を満たしていないと判断する場合
・認証局秘密鍵が危殆化し、機密性が失われた場合又はその可能性があ

る場合
・その他、本認証局が必要と判断する場合

4．9．2　失効の依頼者

証明書発行対象者のみが、本認証局に対して、証明書の失効を依頼できる。
ただし、証明書発行対象者が消防本部の場合、消防本部に加えて、消防庁による失効依頼も許容する。

4．9．3　失効の手続

本認証局は、失効依頼書もしくは失効に関わるWEB申請を受領した場合、以下の処理を行う。
なお、本認証局の判断による失効の場合、以下の（２）及び（３）の処理を行う。

（１）証明書を発行依頼した情報を基に依頼書もしくは失効に関わるWEB申請の確認を行う。
（２）証明書の失効処理を行う。
（３）証明書の失効を依頼する者に失効が完了した旨の通知を行う。

4．9．4　失効依頼までの期間

証明書の失効を依頼する者は、証明書失効の要件に規定した事由が発生した場合は、速やかに失効依頼を行う。

4．9．5　失効処理の期間

本認証局は、失効依頼に記載の失効理由に基づき、速やかに失効処理を行う。

4．9．6　失効情報の確認手段

検証者は、CRL によって検証する対象の証明書が失効されていないか、確認しなければならない。

4．9．7　CRL 発行頻度

本認証局は、失効情報の更新がない場合でも、24 時間ごとに CRL を発行する。発行する CRL の有効期間は、7 日間とする。

4．9．8　CRL 公開までの最大遅延期間

本認証局は CRL の有効期間である 7 日間以内に新たに CRL の公開を行う。

4．9．9　オンラインによる証明書失効状況確認サービスの提供

本認証局は、CRL 以外での失効情報の公開は行わない。

4．9．10　オンラインによる証明書失効状況確認サービス利用の要件

本認証局は、CRL 以外での失効情報の公開は行わないため規定しない。

4．9．11　その他の失効情報確認手段

本認証局は、CRL 以外での失効情報の公開は行わないため規定しない。

4．9．12　認証局秘密鍵が危殆化した際の手順

本認証局は、認証局秘密鍵が危殆化した場合、以下の処理を行う。ただし、認証局秘密鍵が危殆化しているためCRLの発行は行わない。

（１）認証局責任者は確認されている事象を速やかに本認証局運営委員会に報告する。
（２）証明書発行業務を停止する。
（３）有効期限が残っている証明書の失効を行う。
（４）証明書発行対象者に書面で認証局秘密鍵の危殆化及び証明書の失効を通知する。

4．9．13　証明書の一時停止の要件

本認証局は、証明書の一時停止は行わない。

4．9．14　一時停止依頼者

本認証局は、証明書の一時停止は行わないため規定しない。

4．9．15　一時停止依頼の処理手順

本認証局は、証明書の一時停止は行わないため規定しない。

4．9．16　一時停止の期間

本認証局は、証明書の一時停止は行わないため規定しない。

4．10　証明書ステータスの確認サービス

本認証局は、証明書ステータスの確認サービスは行わない。

4．11　証明書の利用終了

証明書の利用を終了する場合は、「4.9 証明書の失効」に規定する失効手続きを行うものとする。

4．12　秘密鍵の預託と鍵回復

本認証局は、発行する証明書に対応する秘密鍵の預託及び鍵回復を行わない。

5　建物、関連設備及び運用に関するセキュリティ

本章は、認証業務を遂行するために必要とされるセキュリティのうち、非技術的なセキュリティについて記述する。

5．1　認証局施設の設備

本節は、登録局端末を除く本認証局の機器が設置してある施設の物理的な設備に関連することについて記述する。

5．1．1　施設の位置と建物構造

本認証局のシステムに係る施設（以下、「本施設」という。）は、地震、火災及び水害、その他の災害による影響を容易に受けない施設に設置する。本施設には、建物構造上、耐震、耐火、水害及び不正侵入防止の措置を講じる。

また、本施設は、建築物の外部及び建築物内に発行局の所在を明示又は暗示する名称を看板もしくは表示板等により一切掲示しない。

5．1．2　認証局設備へのアクセス

本認証局に係る施設は、入退館等に際して資格確認を行い、識別証等により入退出を管理する。

（１）登録局（RA局）

認証業務を行う各室は、業務の重要度に応じたセキュリティレベルを設定し、相応する入退室管理を行う。

（２）発行局（IA局）

入退室時の認証には、各室内において行われる認証業務の重要度に応じ、権限保有者であることを確認できる入退室用カードもしくは生体認証等を用いる。建物内及び各室内は、監視システム及び監視要員による24時間365日監視を行う。

5．1．3　電源及び空調設備

本認証局に係る施設は、機器類の運用のために十分な容量の電源を確保し、また、空調設備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。発行局については、瞬断、停電に備えた対策を講じ、商用電源が供給されない事態においては、自家発電機による電源供給に切り換える。また、空調設備は二重化する。

5．1．4　水害及び地震対策

本認証局に係る施設は、水害による影響を容易に受けない場所に設置する。発行局については、建物及び各室に漏水検知器を設置し、天井、床には防水対策を講じる。

5．1．5　防火対策

本認証局に係る施設は、耐火構造とする。発行局については、本認証局に係るシステムを設置する室は防火区画とし、自動ガス消火設備を備える。

5．1．6　地震に対する予防措置と対策

本施設は、現行の建築基準法に規定する構造上の安全を有する。建物は、新耐震規準に基づいた耐震構造にて設計する。また、本認証局のシステム機器及び什器には転倒及び落下を防止する対策を講じる。

5．1．7　記録媒体

本認証局のシステムのバックアップデータが含まれる媒体、審査業務で使用した書類等については、職務上利用することが許可された者のみが入室できる室内に保管する。また、バックアップ等で作成した記録媒体は、施錠可能なキャビネットで保管する。

5．1．8　廃棄物の処理

本施設は、機密情報を含む書類はシュレッダーにより裁断の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

5．1．9　施設外のバックアップ

本認証局は、不測の事態に備え、認証局秘密鍵を施設外で厳重に保管する。また、本認証局は、施設外のバックアップについては公開しない。

5．2　役割の定義

本節は、本認証局を運営する際に必要な役割の定義及び各者の責任について記述する。

5．2．1　各要因の役割及び責任

本認証局は、認証局を運営するために必要な人員（以下、「認証局要員」という。）及びその役割を以下のとおり定める。

（１）認証局運営委員

本認証局運営委員会において、運営方針等を協議する。

（２）認証局責任者

認証局の運営に係る責任及び執行権限を有する。

（３）認証局副責任者

認証局責任者を補佐し、認証局責任者に事故等があるときは、その職務を代行する。

（４）システム管理者（登録局責任者）

登録局の業務に関する管理責任、作業の承認権限及び認証局の設備に関する管理責任を有する。本認証局の登録局に係る業務を統括し、業務

オペレータを管理する。各窓口の責任者とする。

（５）システム管理補助者

登録局の業務及び認証局の設備に関する職務について、システム管理者を補佐し、システム管理者が不在の場合又はシステム管理者の指示を受けた場合は、その職務の全部又は一部を代行する。

（６）システム管理担当者（登録局オペレータ）

本認証局の登録局に係る業務を行う。

システム管理者の指示の下に、登録局の業務（受付・審査登録）、登録確認業務及び認証局の設備の管理に関する事務を所掌する。

（７）発行局責任者

本認証局の発行局に係る業務を統括し、発行局システムアドミニストレータ及び発行局オペレータを管理する。

（８）発行局システムアドミニストレータ

発行局システムアドミニストレータは、発行局責任者の管理の下、本認証局のシステムの維持・管理を行う。

（９）発行局オペレータ

本認証局に係るシステムの運用、保守及び鍵管理等を行う。

（１０）業務監査担当者

本認証局とは独立した組織で監査を行う。

5．2．2　担当ごとに必要とされる人数

本認証局は、発行局システムアドミニストレータ及び発行局オペレータについては、2 名以上配置する。

5．2．3　個々の役割に対する本人性確認

本認証局は、各役割に応じ、認証業務を行う各室の入室権限及び本認証局のシステムの操作権限を定める。また、発行局に関する各室への入室時又はシステムの操作時においては、入退室カード、生体認証、電子証明書、ID 及びパスワード等の単体又は組合せにより、本人性及び入室・操作権限の確認ならびに認証を行う。

5．2．4　分轄が必要となる役割

本認証局は、下記の職務については、兼務することを認めない。

（１）認証局責任者

（２）登録局責任者

（３）登録局オペレータ

（４）発行局責任者

（５）業務監査担当者

5．3　要員の管理

本節は、要員の資格、経験及び研修等について記述する。

5．3．1　資格、経験及び身分証明に関する要件

本認証業務に従事する認証局要員については、職務規程に基づき、審査、教育、配置転換等を行う。但し、業務の一部が外部の委託会社に委託される場合、当該委託業務に従事する職員は、当該委託会社の職務規程に基づき審査、教育、配置転換等を行う。

5．3．2　経歴の調査手順

認証局要員の適格性は、本認証局の定める規程に従うものとする。

5．3．3　研修

本認証局は、認証局要員に対し、その業務に応じた知識・技術情報の提供又は教育訓練等を行う。

5．3．4　研修の頻度

本認証局は、認証局要員に対する再教育及び訓練を適宜実施する。

また、以下の事態が生じた場合には、教育・訓練を実施する。

（１）本 CP/CPS、及び関連諸規定が改訂され、認証局責任者、発行局責任者、又は登録局責任者が必要と判断した場合。

（２）本認証局システムを変更する場合であって、認証局責任者、発行局責任者、又は登録局責任者が必要と判断した場合。

（３）その他、認証局責任者、発行局責任者、又は登録局責任者が必要と判断した場合。

5．3．5　職務のローテーション

本認証局は、必要に応じて認証局要員の配置転換を行う。

5．3．6　罰則等

認証局要員が過失、故意に関わらず、本 CP/CPS に記載されるポリシーと手続き、もしくは運用手順書に定める手順等に違反した場合、速やかに原因及び影響範囲の調査を行った上で、処罰を課す。

5．3．7　委託契約に関する要件

本認証局は、外部の委託会社に委託された業務に係る職員については、委託先の規則に則った義務を遵守させる。

5．3．8　各要員への資料

本認証局は、認証局要員が、運用手順書等、業務に係るドキュメントをその役割に応じて参照できる措置を講じる。

5．4　監査ログの取り扱い

本節は、監査ログについて記述する。

5．4．1　記録する事象の種類

本認証局は、本 CP/CPS の準拠性及び情報セキュリティ対策の妥当性を評価するために、本認証局における業務及び情報セキュリティに関する重要な事象を対象に、アクセスログや操作ログ等、監査ログを収集する。

5．4．2　監査ログの検査頻度

本認証局は、認証局運用に疑義が生じた際などにおいて、機能不全、脆弱性又は悪意の行動を検出する目的で監査ログを確認する。

5．4．3　監査ログの保存期間

本認証局は、発行した電子証明書の有効期間満了後の少なくとも 1 年間は監査ログを保管する。他の記録については、当該ログ発生より 3 年間保持する。

5．4．4　監査ログの保護

本認証局は、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

5．4．5　監査ログのバックアップ

本認証局は、監査ログに関する電子データを日次でバックアップし取得する。紙媒体については、原本のみを保管する。

5．4．6　収集システム

発行局のシステムは、実装された機能により監査ログを自動的に収集する。

5．4．7　記録した事象の通知

本認証局は、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

5．4．8　脆弱性の検査

本認証局は、本認証局に係るシステムに対し、外部の専門機関による定期的な脆弱性評価を行う。また、その評価結果を文書化し保管する。

5．5　記録の保管

本節は、本認証局における記録の保管・保持方針について記述する。

5．5．1　記録の種類

本認証局は、「5.4.1 記録する事象の種類」で規定された監査ログのほか、以下の情報を保管する。

（１）認証局証明書

（２）加入者・サービス提供者用証明書発行・失効に係る情報
（３）内部監査報告書
（４）本 CP/CPS 及び関連諸規定

5．5．2　記録の保存期間

本認証局は、「5.5.1 記録の種類」に規定される記録について、関連する電子証明書の有効期間を超えて少なくとも 1 年間保管する。

5．5．3　記録の保護

「5.4.4 監査ログの保護」を準用する。

5．5．4　記録のバックアップ

「5.4.5 監査ログのバックアップ」を準用する。

5．5．5　記録のタイムスタンプ

本認証局は、「5.5.1 記録の種類」に関し、帳票類については起票日もしくは処理した日付を記録する。また、日付のみでは記録としての証明力に欠ける場合は、時刻も記録する。本認証局及び加入者・サービス提供者の電子証明書については、発行された日時を記録する。また、本認証局のシステムには、発行する電子証明書及び監査ログに対して正確な日付・時刻を記録するために必要な措置を講じる。

5．5．6　収集システム

本認証局は、電子データについては本認証局に係るシステムの機能により収集する。その他、紙媒体については、認証局要員が収集する。

5．5．7　記録の検証手段

本認証局は、「5.5.1 記録の種類」に関し、記録の取得及び閲覧は、業務監査担当者及び認証局責任者が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

5．6　鍵の切り替え

本認証局は、13年3か月以内に認証局秘密鍵及び自己署名証明書を更新する。

5．7　災害等からの復旧

本節は、災害等が起きた際の通知及び復旧手続きについて記述する。

5．7．1　災害等からの復旧手続

本認証局は、発行局の責による場合を除き、本認証局の秘密鍵の危殆化によるサービスの停止を不可抗力事項として扱い、同サービス再開に要する時間について保証しない。

本認証局は、以下の措置を実施するとともに、加入者・サービス提供者への周知を図る。

（１）危殆化した秘密鍵を用いた認証業務の停止
（２）全ての電子証明書の失効
（３）危殆化の原因調査
（４）本認証局の新しい鍵ペアの生成と対応する電子証明書の発行
（５）本認証業務の再開の妥当性評価
（６）本認証業務の再開
（７）新たな鍵ペアの生成及び電子証明書の発行

本認証局が被災した場合には、「5.7.4 災害等発生時の事業継続性」に基づき、復旧に努める。

5．7．2　ハードウェア等が破損した場合の対処

本認証局は、ハードウェア、ソフトウェア、データが破壊された場合には、バックアップ用のハードウェア、ソフトウェア、データにより、遅滞なく復旧作業を行う。

5．7．3　秘密鍵が危殆化した場合の対処

加入者は、自身の秘密鍵の危殆化又は危殆化が疑われる事態が生じた場合、「4.9 証明書の失効」に記載されたとおり、当該事態の発生を加入者管理組織に連絡し、加入者管理組織の指示又は定めに従うものとする。

5．7．4　災害等発生時の事業継続性

本認証局は、災害による認証局の停止を不可抗力事項として取扱い、サービスの再開に要する時間について保証しない。

本認証局は、災害によりサービスが停止した場合、加入者が閲覧可能なウェブサイトにおいて、その旨公開する。

本認証局を管理する本基金は、以上に掲げる措置を実施するとともに、被災状況の調査を行い、調査結果に基づき、復旧方針を定めるものとし、発行局、登録局は当該復旧方針に従い復旧作業を実施する。

5．8　認証局の廃止

本認証局は、業務を終了する場合、加入者・サービス提供者に事前に通知するほか、加入者が閲覧可能なウェブサイトにおいても、その旨公開する。

本認証局が保有する電子証明書発行・失効申請に関わる情報については、廃棄するものとし、この旨は業務終了時に加入者が閲覧可能なウェブサイトにて告知する。

6　技術的セキュリティ

本章は、認証業務を遂行するために必要とされるセキュリティのうち、技術的なセキュリティについて記述する。

6．1　鍵ペアの生成と実装

本節は、鍵ペア（秘密鍵及び公開鍵）の生成と鍵ペアの導入方法について記述する。

6．1．1　鍵ペアの生成

（１）本認証局の鍵ペアは、認証設備室内で複数人の発行局オペレータの立会いの下、HSM内で生成する。

（２）加入者の鍵ペアは、本認証局において証明書発行時にソフトウェアで生成する。

（３）サービス提供者の鍵ペアは、サービス提供者において生成する場合と本認証局において証明書発行時にソフトウェアで生成する場合がある。

6．1．2　証明書発行対象者への秘密鍵の送付

加入者・サービス提供者の秘密鍵は、本認証局内で生成し暗号化した状態で提供する。

本認証局は、加入者が証明書を取得するための情報を、配達状況を確認できる方法（書留や簡易書留等）で送付する。証明書の取得は SSL 暗号化通信により行う。ただし、加入者が消防本部の場合、消防庁が加入者のメールアドレスの真正性の確認を実施していることから、当該メールアドレスに証明書を取得するための情報を送付する。

6．1．3　認証局への公開鍵の送付

本認証局は、加入者・サービス提供者からの公開鍵の配送を受け付けない。

6．1．4　検証者への認証局公開鍵の配布

本認証局は、検証者に対し認証局の公開鍵を配布する。

6．1．5　鍵のサイズ

本認証局で発行する証明書において使用するアルゴリズム及び鍵のサイズは以下のとおりとする。

（１）自己署名証明書

公開鍵アルゴリズム：RSA Encryption

鍵のサイズ：2048bit

（２）利用者証明書、サーバ証明書、コード署名証明書及びタイムスタンプ証明書

公開鍵アルゴリズム：RSA Encryption

鍵のサイズ：2048bit

6．1．6　公開鍵パラメータの生成

本認証局の公開鍵パラメータは、HSM で生成する。

6．1．7　鍵の利用目的

鍵の利用目的は「7.1 証明書のプロファイル」に規定する Key Usage（鍵用途）とする。

6．2　秘密鍵の保護

本節は、秘密鍵の生成から廃棄までの管理方法について記述する。

6．2．1　暗号モジュールの評価基準

認証局秘密鍵の生成及び保管を行う暗号モジュールは、FIPS 140-2 レベル 3 の認定を取得した HSM を使用する。

6．2．2　秘密鍵の複数人による管理

認証局秘密鍵の生成等の管理は、常時複数人の発行局システムアドミニストレータが行う。

6．2．3　秘密鍵の預託

本認証局は、秘密鍵の預託を行わない。

6．2．4　秘密鍵のバックアップ

認証局秘密鍵のバックアップは、常時複数人の発行局オペレータが行う。HSM からバックアップした本認証局の秘密鍵は、暗号化して複数に分割し、施錠可能な保管庫にて安全に保管する。

6．2．5　秘密鍵の保管

認証局秘密鍵は、常時複数人の発行局オペレータが行う。本認証局の秘密鍵は、暗号化して複数に分割し、施錠可能な保管庫にて安全に保管する。

6．2．6　暗号モジュールへの秘密鍵の復元

本認証局は、HSM の故障など秘密鍵の復元が必要な場合、発行局責任者の管理・指示の下、発行局システムアドミニストレータ及び発行局オペレータが、バックアップからの秘密鍵の復元を行う。このとき、バックアップデータを本施設外へ移送しない。

6．2．7　暗号モジュールへの秘密鍵の格納

認証局秘密鍵は、FIPS 140-2 レベル 3 の HSM によって生成し、暗号化された状態で格納する。

6．2．8　秘密鍵の活性化方法

本認証局の秘密鍵は、本認証局起動手順に従い、発行局責任者の管理の下、複

数人の発行局システムアドミニストレータが活性化を行う。また、活性化作業の内容を記録する。

6．2．9　秘密鍵の非活性化方法

本認証局の秘密鍵は、本認証局停止手順に従い、発行局責任者の管理の下、複数人の発行局システムアドミニストレータが非活性化を行う。また、非活性化作業の内容を記録する。

6．2．10　秘密鍵の廃棄方法

本認証局の秘密鍵は、認証局責任者の指示を受け、発行局責任者の管理の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータが破壊する。同時に、バックアップされたデータについても、同様の手順に基づき破壊する。また、破壊作業の内容を記録する。

6．2．11　暗号モジュールの能力

本認証局の HSM は、暗号モジュールの評価基準である FIPS 140-2 レベル 3 の認定を取得しているものを用いることにより同レベルの能力を有する。

6．3　鍵ペア管理に関するその他の留意事項

6．3．1　公開鍵の保管

公開鍵の保存については、それを含む電子証明書を保存することによって行う。

6．3．2　公開鍵証明書の有効期間及び鍵ペアの使用期間

本認証局で発行する証明書の有効期間及び鍵ペアの使用期間は以下のとおりとする。

（１）自己署名証明書
　　証明書有効期間：13年3か月
　　鍵ペア使用期間：13年3か月
（２）利用者証明書
　　証明書有効期間：3年3か月
　　鍵ペア使用期間：3年3か月
（３）サーバ証明書
　　証明書有効期間：3年3か月
　　鍵ペア使用期間：3年3か月
（４）コード署名証明書
　　証明書有効期間：3年3か月
　　鍵ペア使用期間：3年3か月
（５）タイムスタンプ証明書
　　証明書有効期間：10年

鍵ペア使用期間：10年

6．4　活性化データ

本節は、活性化データの生成・保護等について記述する。活性化データとは、証明書の秘密鍵を利用可能な状態にするためのデータである。

6．4．1　活性化データの生成

認証局自身の秘密鍵の活性化データは、認証設備室内においてHSM内で生成され、専用のハードウェアで安全に管理する。

証明書発行対象者の秘密鍵の活性化データは、加入者が暗号化された証明書を復号化する際に利用するパスワードである。この活性化データは、本認証局で証明書を発行する際に容易に推測されないものを生成する。

ただし、サービス提供者からの証明書要求ファイルによる証明書作成の場合、サービス提供者が容易に推測されないものを生成することとし、本認証局は管理しない。

6．4．2　活性化データの保護

認証局秘密鍵の活性化データは、認証設備室内で安全に保護する。
利用者証明書、コード署名証明書及びタイムスタンプ証明書の秘密鍵の活性化データは、加入者及び当該サービス提供者へ伝えた後、認証局においては保管しないものとする。

また、伝えられた活性化データは、加入者により安全に保護されるものとする。

サーバ証明書の活性化データは、サービス提供者により安全に保護されるものとする。

6．4．3　活性化データのその他の要件

証明書発行対象者が活性化データを紛失等した場合、本認証局は再度活性化データを通知することはしない。

6．5　コンピュータのセキュリティ管理

本節は、本認証局で使用するコンピュータのセキュリティ管理について記述する。

6．5．1　特定のコンピュータセキュリティに関する技術的要件

本認証局に係るシステムは、アクセス制御機能、操作者である発行局オペレータの識別と認証機能、システムのバックアップ・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の評価

本認証局に係るシステムは、事前に導入評価を実施し、認証業務開始後もセキ

ュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

6．6　システムのライフサイクル管理

6．6．1　システム開発管理

本認証局の構築・修正・変更は、認証局責任者の管理の下、信頼できる組織及び環境にて作業を実施する。修正・変更に際しては、テスト環境において検証を行い、認証局責任者の承認を得た上で導入する。ただし、軽微な修正・変更の場合、発行局については発行局責任者の承認の下、登録局については登録局オペレータの判断により、作業を実施する。

6．6．2　セキュリティ運用管理

本認証局に係るシステムは、十分なセキュリティレベルを確保するために必要な設定を行う。また、システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行ない、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

6．6．3　ライフサイクルのセキュリティ管理

本認証局のシステムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画又は手順を策定・評価し、必要に応じ試験を行う。また、各作業の内容を記録する。

6．7　ネットワークのセキュリティ管理

本認証局のシステムとインターネット等の外部システムとは、ファイアウォール等を介して接続し、また侵入検知システムによる監視を行う。

6．8　タイムスタンプ

本認証局に係るシステムには、発行する電子証明書及び監査ログ等に対して正確な日付・時刻を記録するために必要な措置を講じる。

7　証明書、CRL 等のプロファイル

本章は、本認証局が発行する証明書及び CRL 等に設定する各領域の値について記述する。

7．1　証明書のプロファイル

本節は、証明書のフォーマット、拡張領域を含む各領域の値について記述する。

7．1．1　バージョン番号

本認証局が発行する証明書は、ITU-T X.509 Version 3 フォーマット証明書形式に準じて作成する。

7．1．2　証明書の拡張領域

証明書の拡張領域のプロファイルは、証明書拡張領域（Extensions）に記載するとおりとする。

7．1．3　アルゴリズムオブジェクト識別子

（１）証明書の基本領域の署名（Signature）アルゴリズム
SHA256 with RSA Encryption （1.2.840.113549.1.1.11）

（２）証明書の基本領域の主体者公開鍵情報アルゴリズム
RSA Encryption （1.2.840.113549.1.1.1）

7．1．4　識別名の形式

証明書の発行者（Issuer）と主体者（Subject）の識別名の形式は「３．１ 識別名」に規定するとおりとする。

7．1．5　名称の制約

本認証局は、証明書に対して名称の制約（Name Constraints）は使用しない。

7．1．6　証明書ポリシー

本認証局は、証明書に対して証明書のポリシー（Certificate Policies）は使用しない。

7．1．7　ポリシーの制約

本認証局は、証明書ポリシーを使用しないため、ポリシーの制約（Policy Constraints）は使用しない。

7．1．8　ポリシーの修飾子

本認証局は、証明書ポリシーを使用しないため、ポリシーの修飾子（Policy Qualifiers）は使用しない。

7．1．9　証明書ポリシーの拡張フィールド

本認証局は、証明書ポリシーを使用しないため、証明書ポリシーの拡張フィールドは使用しない。

7．1．10　拡張キー

本認証局は、タイムスタンプ証明書に拡張キーの使用目的を設定する。

表５．自己署名証明書

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）1	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。 YYMMDDHHMMSSZ
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。 YYMMDDHHMMSSZ
Subject	－	cn = Online Billing NW	本認証局の識別名

領域名	C	値	説明
（主体者）		Common Root CA - G* o = Online Billing NW System c = JP	（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Subject Public Key Info （主体者公開鍵情報）	ー		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		自己署名証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。

領域名		C	値	説明
	Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier（主体者鍵識別子）		F		自己署名証明書の公開鍵を識別するための情報を表す。
	Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
BasicConstraints（基本制約）		T		
	CA		True	認証局の証明書であることを表す。Internet Explorer では「Subject Type=CA」と表示される。
Key Usage（鍵用途）		T	000001100（2 進数表記）	鍵の使用目的を設定する。
	Digital Signature		0	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
	Non Repudiation		0	否認防止用の署名検証ができる。
	Key Encipherment		0	共通鍵等の鍵を暗号化できる。
	Data Encipherment		0	データを直接暗号化できる。
	Key Agreement		0	鍵は鍵交換ができる。
	Key Cert Sign		1	証明書の CA 署名の検証ができる。
	CRL Sign		1	CRL 署名の検証ができる。
	Encipher Only		0	交換した鍵でデータを暗号化できる。（Key Agreement がセットされている場合の

領域名		C	値	説明
				み指定可）
	Decipher Only		0	交換した鍵でデータを復号化できる。（Key Agreement がセットされている場合のみ指定可）
Issuer's Signature（発行者署名）		－		証明書に付与した署名の値を示す。
	Algorithm Identifier（アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
	Encrypted		※署名値	証明書に付与した署名の値を示す。

表６．利用者証明書（医療保険者等向け中間サーバ等システム）

領域名		C	値	
Version（バージョン番号）		－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number（シリアル番号）		－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature（署名アルゴリズム）		－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
	Algorithm Identifier（アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer（発行者）		－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。

領域名	C	値	
			- G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UCT Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UCT Time 型
Subject （主体者）	－	（例） cn = 99999999 ou = insurance o = IntermediateServer c = JP	医療保険者等の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）	－		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		利用者証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッ	自己署名証明書の公開鍵の SHA1 によるハッシュ

領域名		C	値	
			シュ値	値を示す。
	Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
	Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier（主体者鍵識別子）		F		利用者証明書の公開鍵を識別するための情報を表す。
	Key Identifier		※利用者証明書の公開鍵の SHA1 によるハッシュ値	利用者証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage（鍵用途）		T	101000000（2 進数表記）	鍵の使用目的を設定する。
	Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
	Non Repudiation		0	否認防止用の署名検証ができる。
	Key Encipherment		1	共通鍵等の鍵を暗号化できる。
	Data Encipherment		0	データを直接暗号化できる。
	Key Agreement		0	鍵は鍵交換ができる。
	Key Cert Sign		0	証明書の CA 署名の検証ができる。
	CRL Sign		0	CRL 署名の検証ができる。

領域名	C	値	
Encipher Only		0	交換した鍵でデータを暗号化できる。(Key Agreement がセットされている場合のみ指定可)
Decipher Only		0	交換した鍵でデータを復号化できる。(Key Agreement がセットされている場合のみ指定可)
Extended Key Usage (拡張鍵用途)	F		鍵の拡張使用目的を設定する。
Key Purpose Id		id-kp-clientAuth	TLS Web クライアント認証を示す。
Certificate Policies	F		
Policy Identifier		0.2.440.200317.1.1.1 (社会保険診療報酬支払基金) 0.2.440.200318.1.1.1 (国民健康保険中央会)	CPS を表す OID の値を示す。
Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points (CRL 配布点)	F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する URI を示す。
Issuer's Signature (発行者署名)	ー		証明書に付与した署名の値を示す。
Algorithm Identifier (アルゴリズム識別子)		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Encrypted		※署名値	証明書に付与した署名の値を示す。

表７．利用者証明書（オンライン請求システム、オンライン資格確認等システム）

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UCT Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UCT Time 型
Subject （主体者）	－	（例） cn = 1310000001 ou ＝ medical ou = Tokyo o = ReceiptOnline c = JP	左の例は東京都の医療機関（医科）の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8

領域名		C	値	説明
				String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）		－		証明書の公開鍵アルゴリズムを示す。
	Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
	Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
	Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）				
Authority Key Identifier （認証局鍵識別子）		F		利用者証明書の署名の検証に使用する証明書を識別するための情報を表す。
	Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
	Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
	Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型

領域名	C	値	説明
Subject Key Identifier （主体者鍵識別子）	F		利用者証明書の公開鍵を識別するための情報を表す。
Key Identifier		※利用者証明書の公開鍵の SHA1 によるハッシュ値	利用者証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage （鍵用途）	T	101000000（2 進数表記）	鍵の使用目的を設定する。
Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
Non Repudiation		0	否認防止用の署名検証ができる。
Key Encipherment		1	共通鍵等の鍵を暗号化できる。
Data Encipherment		0	データを直接暗号化できる。
Key Agreement		0	鍵は鍵交換ができる。
Key Cert Sign		0	証明書の CA 署名の検証ができる。
CRL Sign		0	CRL 署名の検証ができる。
Encipher Only		0	交換した鍵でデータを暗号化できる。 （Key Agreement がセットされている場合のみ指定可）
Decipher Only		0	交換した鍵でデータを復号化できる。 （Key Agreement がセットされている場合のみ指定可）
Certificate Policies	F		
-		0.2.440.200317.1.1.1 （社会保険診療報酬支	CPS を表す OID の値を示す。

領域名	C	値	説明
		払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	
		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）	F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する URI を示す。
Issuer's Signature （発行者署名）	－		証明書に付与した署名の値を示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Encrypted		※署名値	証明書に付与した署名の値を示す。

表８．サーバ証明書（医療保険者等向け中間サーバ等システム）

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。

領域名	C	値	説明
Issuer （発行者）	ー	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	ー		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UTC Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UTC Time 型
Subject （主体者）	ー	（例） cn = www.mi.miis.jp ou = Server o = Intermediate Server c = JP	サーバーの識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）	ー		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		サーバ証明書の署名の検証に使用する証明書を識別するための情報

領域名	C	値	説明
			を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		ou = Online Billing NW Common Root CA o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier（主体者鍵識別子）	F		サーバ証明書の公開鍵を識別するための情報を表す。
Key Identifier		※サーバ証明書の公開鍵の SHA1 によるハッシュ値	サーバ証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage（鍵用途）	T	101000000（2 進数表記）	鍵の使用目的を設定する。
Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
Non Repudiation		0	否認防止用の署名検証ができる。
Key Encipherment		1	共通鍵等の鍵を暗号化できる。
Data Encipherment		0	データを直接暗号化できる。
Key Agreement		0	鍵は鍵交換ができる。
Key Cert Sign		0	証明書の CA 署名の検証ができる。
CRL Sign		0	CRL 署名の検証ができる。

領域名	C	値	説明
Encipher Only		0	交換した鍵でデータを暗号化できる。 （Key Agreement がセットされている場合のみ指定可）
Decipher Only		0	交換した鍵でデータを復号化できる。 （Key Agreement がセットされている場合のみ指定可）
Extended Key Usage （拡張鍵用途）	F		鍵の拡張使用目的を設定する。
Key Purpose Id		id-kp-serverAuth	TLS Web サーバ認証を示す。
Certificate Policies	F		
Policy Identifier		0.2.440.200317.1.1.1 （社会保険診療報酬支払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	CP を表す OID の値を示す。
Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）	F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する場所を示す。
Subject Alternative Name （サブジェクト代替名（SAN））	F	（例） DNS Name = www.abc.rece	SAN の DNS Name の値でアクセスするドメインとの一致を判定する動作となっているブラウザ で、SAN の設定がないことによる「プライバシーエラー」等の表示を抑止する。設定する値は、Common Name と同一とする。

領域名	C	値	説明
Issuer's Signature （発行者署名）	－		証明書に付与した署名の値を示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Encrypted		※署名値	証明書に付与した署名の値を示す。

表９．サーバ証明書（オンライン請求システム、オンライン資格確認等システム）

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。

領域名	C	値	説明
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UTC Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UTC Time 型
Subject （主体者）	－	（例） cn = www.abc.rece ou = Server o = ReceiptOnline c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）	－		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		サーバ証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の

領域名	C	値	説明
			世代を記載する。
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier（主体者鍵識別子）	F		サーバ証明書の公開鍵を識別するための情報を表す。
Key Identifier		※サーバ証明書の公開鍵の SHA1 によるハッシュ値	サーバ証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage（鍵用途）	T	101000000（2 進数表記）	鍵の使用目的を設定する。
Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
Non Repudiation		0	否認防止用の署名検証ができる。
Key Encipherment		1	共通鍵等の鍵を暗号化できる。
Data Encipherment		0	データを直接暗号化できる。
Key Agreement		0	鍵は鍵交換ができる。
Key Cert Sign		0	証明書の CA 署名の検証ができる。
CRL Sign		0	CRL 署名の検証ができる。
Encipher Only		0	交換した鍵でデータを暗号化できる。（Key Agreement がセットされている場合のみ指定可）

領域名	C	値	説明
Decipher Only		0	交換した鍵でデータを復号化できる。 （Key Agreement がセットされている場合のみ指定可）
Certificate Policies	F		
Policy Identifier		0.2.440.200317.1.1.1 （社会保険診療報酬支払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	CP を表す OID の値を示す。
Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）	F	http://crldownload.obn.managedpki.ne.jp/crl/rsvr_cdp.crl	CRL を配布する場所を示す。
Subject Alternative Name （サブジェクト代替名（SAN））	F	（例） DNS Name = www.abc.rece	SAN の DNS Name の値でアクセスするドメインとの一致を判定する動作となっているブラウザで、SAN の設定がないことによる「プライバシーエラー」等の表示を抑止する。設定する値は、Common Name と同一とする。
Issuer's Signature （発行者署名）	ー		証明書に付与した署名の値を示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Encrypted		※署名値	証明書に付与した署名の値を示す。

表１０．コード署名証明書（医療保険者等向け中間サーバ等システム）

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。 UCT Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。 UCT Time 型
Subject （主体者）	－	（例） cn = Online Billing NW Application Developer ou =insurance o= ReceiptOnline	コード署名を行ったサービス提供者の識別名（DN）を示す。 Country 属性のみ Printable String 型を

領域名	C	値	説明
		c = JP	使用する。それ以外は UTF8 String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）	－		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		コード署名証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier （主体者鍵識別子）	F		コード署名証明書の公開鍵を識別するための情報を表す。

領域名		C	値	説明
	Key Identifier		※コード署名証明書の公開鍵の SHA1 によるハッシュ値	コード署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage（鍵用途）		T	100000000（2 進数表記）	鍵の使用目的を設定する。
	Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
	Non Repudiation		0	否認防止用の署名検証ができる。
	Key Encipherment		0	共通鍵等の鍵を暗号化できる。
	Data Encipherment		0	データを直接暗号化できる。
	Key Agreement		0	鍵は鍵交換ができる。
	Key Cert Sign		0	証明書の CA 署名の検証ができる。
	CRL Sign		0	CRL 署名の検証ができる。
	Encipher Only		0	交換した鍵でデータを暗号化できる。(Key Agreement がセットされている場合のみ指定可)
	Decipher Only		0	交換した鍵でデータを復号化できる。(Key Agreement がセットされている場合のみ指定可)
Extended Key Usage（拡張鍵用途）		F		鍵の拡張使用目的を設定する。
	Key Purpose Id		id-kp-codeSigning	TLS Web クライアント認証を示す。
Certificate Policies		F		

領域名		C	値	説明
	Policy Identifier		0.2.440.200317.1.1.1 （社会保険診療報酬支払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	CPS を表す OID の値を示す。
	Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）		F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する場所を示す。
Issuer's Signature （発行者署名）		－		証明書に付与した署名の値を示す。
	Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
	Encrypted		※署名値	証明書に付与した署名値を示す。

表１１．コード署名証明書（オン請求・オン資格システム）

領域名		C	値	説明
Version （バージョン番号）		－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）		－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）		－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
	Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。

領域名	C	値	説明
Issuer （発行者）	―	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	―		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UCT Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UCT Time 型
Subject （主体者）	―	（例） Online Billing NW Application Developer ou = support o= ReceiptOnline c = JP	コード署名を行ったサービス提供者の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。
Subject Public Key Info （主体者公開鍵情報）	―		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型

Extensions （証明書拡張領域）			
領域名	C	値	説明
Authority Key Identifier （認証局鍵識別子）	F		コード署名証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Subject Key Identifier （主体者鍵識別子）	F		コード署名証明書の公開鍵を識別するための情報を表す。
Key Identifier		※コード署名証明書の公開鍵の SHA1 によるハッシュ値	コード署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage （鍵用途）	T	100000000（2 進数表記）	鍵の使用目的を設定する。
Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
Non Repudiation		0	否認防止用の署名検証ができる。
Key Encipherment		0	共通鍵等の鍵を暗号化

				できる。
	Data Encipherment		0	データを直接暗号化できる。
	Key Agreement		0	鍵は鍵交換ができる。
	Key Cert Sign		0	証明書の CA 署名の検証ができる。
	CRL Sign		0	CRL 署名の検証ができる。
	Encipher Only		0	交換した鍵でデータを暗号化できる。 （Key Agreement がセットされている場合のみ指定可）
	Decipher Only		0	交換した鍵でデータを復号化できる。 （Key Agreement がセットされている場合のみ指定可）
Certificate Policies		F		
	Policy Identifier		0.2.440.200317.1.1.1 （社会保険診療報酬支払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	CPS を表す OID の値を示す。
	Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）		F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する場所を示す。
Issuer's Signature （発行者署名）		ー		証明書に付与した署名の値を示す。
	Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
	Encrypted		※署名値	証明書に付与した署名の値を示す。

表１２．タイムスタンプ証明書（オン請求・オン資格システム）

領域名	C	値	説明
Version （バージョン番号）	－	2	証明書形式のバージョンが X.509 のバージョン 3 であることを示す。Integer 型
Serial Number （シリアル番号）	－	（例）10	証明書のシリアル番号を示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Validity （証明書正当有効期間）	－		証明書の正当な有効期間を示す。
Not Before （発行日）		（例）190101000000Z	証明書の有効期間開始日を示す。UCT Time 型
Not After （終了日）		（例）260101000000Z	証明書の有効期間終了日を示す。UCT Time 型
Subject （主体者）	－	（例） Online Billing NW Application Developer ou = support	タイムスタンプを行ったサービス提供者の識別名（DN）を示す。 Country 属性のみ

領域名	C	値	説明
		o= ReceiptOnline c = JP	Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 commonName の値は任意の値を指定。
Subject Public Key Info （主体者公開鍵情報）	－		証明書の公開鍵アルゴリズムを示す。
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.1	証明書の公開鍵アルゴリズム識別子である、RSA Encryption を表す OID の値を示す。
Parameter （パラメータ）		NULL	RSA の場合、本項目には値が設定されない。
Public Key （公開鍵）		※公開鍵の値	証明書の公開鍵の値を示す。Bit String 型
Extensions （証明書拡張領域）			
Authority Key Identifier （認証局鍵識別子）	F		タイムスタンプ証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。

領域名	C	値	説明
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Extended Key Usage	T		拡張キーの使用目的を設定する。また、「critical」を指定する。
Time Stamp		1.3.6.1.5.5.7.3.8	timeStamping
Subject Key Identifier（主体者鍵識別子）	F		タイムスタンプ証明書の公開鍵を識別するための情報を表す。
Key Identifier		※タイムスタンプ証明書の公開鍵の SHA1 によるハッシュ値	タイムスタンプ証明書の公開鍵の SHA1 によるハッシュ値を示す。
Key Usage（鍵用途）	T	100000000（2 進数表記）	鍵の使用目的を設定する。
Digital Signature		1	「Key Cert Sign」「CRL Sign」の目的を除くデジタル署名の検証ができる。
Non Repudiation		0	否認防止用の署名検証ができる。
Key Encipherment		0	共通鍵等の鍵を暗号化できる。
Data Encipherment		0	データを直接暗号化できる。
Key Agreement		0	鍵は鍵交換ができる。
Key Cert Sign		0	証明書の CA 署名の検証ができる。
CRL Sign		0	CRL 署名の検証ができる。
Encipher Only		0	交換した鍵でデータを暗号化できる。（Key Agreement がセットされている場合のみ指定可）

領域名		C	値	説明
	Decipher Only		0	交換した鍵でデータを復号化できる。 （Key Agreement がセットされている場合のみ指定可）
Certificate Policies		F		
	Policy Identifier		0.2.440.200317.1.1.1 （社会保険診療報酬支払基金） 0.2.440.200318.1.1.1 （国民健康保険中央会）	CPS を表す OID の値を示す。
	Policy Qualifiers		https://cert.obn.managedpki.ne.jp/p/c	CPS の URI を示す。
CRL Distribution Points （CRL 配布点）		F	http://crldownload.obn.managedpki.ne.jp/crl/cdp.crl	CRL を配布する場所を示す。
Issuer's Signature （発行者署名）		－		証明書に付与した署名の値を示す。
	Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
	Encrypted		※署名値	証明書に付与した署名の値を示す。

補足事項 C：クリティカルフラグ、F：FALSE、T：TRUE を意味する。

7．2　CRL プロファイル

本節は、CRL のフォーマット、拡張領域を含む各領域の値について記述する。

7．2．1　バージョン番号

本認証局が発行する CRL は ITU-T X.509 version 2 CRL フォーマット形式に準じて作成する。

7．2．2　CRL の拡張領域

CRL の拡張領域のプロファイルは「証明書失効リスト」の証明書失効リスト拡張（CRL Extensions）に記載するとおりとする。

表１３．　証明書失効リスト

領域名	C	値	説明
Version （バージョン番号）	－	1	失効リスト形式のバージョンが X.509 のバージョン2 であることを示す。Integer 型
Signature （署名アルゴリズム）	－		認証局が発行する証明書に署名を施す際に使用した署名アルゴリズム
Algorithm Identifier （アルゴリズム識別子）		1.2.840.113549.1.1.11	SHA256 with RSA Encryption を表す OID の値を示す。
Issuer （発行者）	－	cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
This Update （今回の更新日）	－	（例）070115200000Z	証明書の有効期間開始日を示す。UTC Time 型
Next Update （次回の更新日）	－	（例）070122200000Z	証明書の有効期間終了日を示す。UTC Time 型
Revocated Certificates （失効した証明書）	－		失効された証明書エントリ
User Certificate		（例）08	失効された証明書のシリアル番号。Integer 型
Revocation Date		（例）070115200000Z	失効日時。UTC Time 型

領域名	C	値	説明
Public Key （公開鍵）			失効証明書ごとの拡張領域
Reason Code	F		失効理由を示すコード
Cessation Of Operation		5	運用停止
Invalidity Date	F	（例）070115200000Z	証明書が実際に無効になった日時。 Generalized Time 型
CRL Extensions （証明書失効リスト拡張）			
Authority Key Identifier （認証局鍵識別子）	F		サーバ証明書の署名の検証に使用する証明書を識別するための情報を表す。
Key Identifier		※自己署名証明書の公開鍵の SHA1 によるハッシュ値	自己署名証明書の公開鍵の SHA1 によるハッシュ値を示す。
Authority Cert Issuer		cn = Online Billing NW Common Root CA - G* o = Online Billing NW System c = JP	本認証局の識別名（DN）を示す。 Country 属性のみ Printable String 型を使用する。それ以外は UTF8 String 型を使用する。 - G*は認証局秘密鍵の世代を記載する。
Authority Cert Serial Number		（例）1	自己署名証明書の証明書のシリアル番号を示す。Integer 型
CRL Number （CRL 番号）	F	（例）5	自己署名証明書の証明書のシリアル番号を示す。Integer 型
Issuer's Signature （発行者署名）	－		証明書に付与した署名の値を示す。
Algorithm Identifier （アルゴリズム識別		1.2.840.113549.1.1.11	SHA2 with RSA Encryption を表す OID の値を示す。

領域名		C	値	説明
	子）			
	Encrypted		※署名値	証明書に付与した署名の値を示す。

7．2．3　基本領域の署名（Signature）アルゴリズム

SHA256 with RSA Encryption （1.2.840.113549.1.1.11）とする。

7．2．4　識別名の形式

CRL の発行者（Issuer）の識別名の形式は「3.1.1 識別名の形式」に規定するとおりとする。

7．3　OCSP プロファイル

本認証局は OCSP を使用しないため、プロファイルの定義は行わない。

8　監査

本章は、監査について記述する。

8．1　監査の頻度と要件

監査は、1 年に 1 度の頻度で定期監査を行う。また、認証業務に疑義が生じた場合、発行局及び登録局の全部又は一部について、「8.2 監査者の身元・資格」に定める監査人が必要と判断した際に監査を実施することができる。

8．2　監査者の身元・資格

本認証局の監査は、必要な知識と経験を有する者が行う。

8．3　監査者と被監査者の関係

公正な監査を遂行するために、監査人は本認証局から独立していることとする。

8．4　監査の項目

本認証局の認証業務が、本 CP/CPS に準拠して実施されていることの監査を範囲とする。

8．5　監査指摘事項への対応

監査により発見された指摘事項は、本認証局運営委員会へ報告する。監査人、認証局責任者、発行局責任者、又は登録局責任者により是正措置が必要と判断された場合、発行局責任者又は登録局責任者の管理の下、是正措置を実施する。

8．6　監査結果の通知

本認証局は、監査結果を加入者・サービス提供者及び署名検証者へ開示しない。
本認証局は、本認証局が必要と認めた対象にのみ監査結果を開示する。

9　他の事項

本章は、その他の業務に関する事項、財務上の責任及び法務上の事項等について記述する。

9．1　料金

本節は、本認証局が提供する証明書及びその他サービスの料金について記述する。

9．1．1　証明書の発行又は更新料

中間サーバ用証明書及び消防庁/消防本部向け証明書の発行又は更新に係る料金は、別途定める。

オン請求・オン資格用証明書は、電子証明書の発行（更新）の際には、電子証明書費用として 1,500 円と郵送手数料 792 円（消費税含む）とする。また、電子証明書費用は、3 年ごとに見直しを行う。

電子証明書を発行した月の翌々月に、利用者が指定した方法により請求する。

電子証明書発行料の納付は、以下のいずれかとする。

（１）診療（調剤）報酬支払額からの控除

電子証明書発行月の翌々月の診療（調剤）報酬から控除し、「当座口振込通知書」により通知する。診療（調剤）報酬の支払額が控除額を下回ることにより控除できなかった場合は、翌月の診療（調剤）報酬から控除することとするが、翌月の支払でも控除できない場合は、電子証明書発行月の３か月後の１０日頃に払込請求書により請求する。

（２）払込請求書による振込み

電子証明書発行月の翌々月１０日頃に利用者あてに「払込請求書」を送付。当該払込請求書に記載する日までに振込み。

なお、電子証明書の発行（更新）に必要な費用を所定の支払期日が過ぎてもなお支払わない場合、当該電子証明書は失効されるものとする。

9．1．2　証明書の参照料

本認証局は証明書の公開は行わないため、料金は発生しない。

9．1．3　CRL の参照料

料金は発生しない。

9．1．4　その他のサービスに対する料金

その他のサービスに対する料金については、必要に応じて別途定める。

9．1．5　払戻し指針

払戻しは行わない。

9．2　財務上の責任

本節は、本認証局の財務上の責任について記述する。

9．2．1　保険の適用範囲

本認証局は、各証明書発行対象者の過失等から生じる損害を補償するための保険に加入しない。

9．2．2　資産

本認証局は、その運営主体である社会保険診療報酬支払基金及び国民健康保険中央会が運営するための十分な財務的基盤を維持するものとする。

9．2．3　証明書発行対象者に対する保険

本認証局は、証明書発行対象者に対する保険の用意はしない。

9．3　機密情報の保護

本節は、秘密として取扱いを行う情報について記述する。

9．3．1　機密情報の範囲

本認証局は、明示的に秘密情報として取り扱わない情報に規定したものを除き、秘密情報の対象として扱うものとする。

また、個人情報については、「9.4 個人情報の保護」で規定する。

9．3．2　秘密情報として取り扱わない情報

証明書、CRL及び本CP/CPSに含まれている情報は、秘密情報として扱わない。その他、以下の情報も秘密情報として扱わない。

（１）本認証局以外から公知となった情報

（２）開示に関して、証明書発行対象者によって承認されている情報

9．3．3　第三者への開示

「9.1.1 証明書の発行又は更新料」に関わらず、本認証局は、弁護士、公認会計士もしくは税理士等の専門家、業務の全部もしくは一部を委託する特定の第三者、裁判所、行政当局、その他の法令・規則等に基づき開示を求める権限を有する者から機密情報の開示を求められた場合は、当該機密情報を開示することができる。

9．3．4　機密情報を保護する責任

本認証局は、秘密情報を保護するため、内部及び外部からの情報漏えいに係る脅威に対して合理的な保護対策を実施する責任を負う。

9．4　個人情報の保護

本節は、個人情報の保護について記述する。

9．4．1　個人情報の保護方針

個人情報は、本CP/CPSに定める事業を遂行するためにのみ利用する。

また、法令等に基づく場合を除き、事前の承認なく個人情報を第三者への開示・提供は行わない。

9．4．2　個人情報として保護する情報

本認証局は、以下の情報は保護すべき個人情報として取り扱う。

（１）各種依頼書に記載された依頼者の個人情報及び付随する情報。

（２）社会保険診療報酬支払基金及び国民健康保険中央会が所有する加入者の情報に含まれる個人情報及び付随する情報。

（３）その他、認証局業務を行う上で、知り得た加入者及びサービス提供者の個人情報及び付随する情報。

9．4．3　個人情報として扱わない情報

本認証局は、個人情報として保護する情報に規定する情報以外は個人情報として取り扱わない。

9．4．4　個人情報を保護する責任

本認証局は、個人情報を保護するため、合理的な保護対策を実施する責任を負う。

9．4．5　個人への通知及び同意

本認証局は、運用上必要となる業務の利用目的に限り、個人情報を利用する。それ以外の個人情報の利用については、法令で除外されているものを除き、本人の同意を得るものとする。

9．4．6　司法手続に基づく開示

本認証局は、法に基づく司法手続き又は行政手続きにより情報開示が求められた場合には、情報を開示することができる。

9．4．7　その他の情報公開示条件

個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、社会保険診療報酬支払基金及び国民健康保険中央会で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費等については、情報開示を求める者の負担とする。

9．5　知的財産権

本認証局と加入者又はサービス提供者との間で別段の合意がない限り、本認証局が提供する情報等は、証明書発行対象者に発行した証明書、秘密鍵及び公開鍵を除いてすべて本認証局に帰属する財産である。

9．6　関係者の責務

本節は、本認証局の関係者が運用を行う上で表明する保証内容について記述する。

9．6．1　認証局の責務

本 CP/CPS に基づき、提供するサービスと運用のすべてについて責任を果たすものとする。

9．6．2　加入者の責務

本 CP/CPS に基づき、加入者は以下の責任を果たすものとする。

（１）証明書発行依頼内容に対する責任

証明書発行依頼を行う場合、本認証局に提示する依頼内容が虚偽なく正確であることに対する責任を負うこと。

（２）証明書記載事項に対する責任

証明書の記載内容について証明書受領時に内容の確認を行い、依頼内容と相違ないことを確認すること。記載内容に誤りがある場合は速やかに当該証明書の失効手続きを行うこと。

（３）秘密鍵等の管理責任

秘密鍵を保護し、紛失、暴露、改ざん又は盗用されることを防止するために適切な措置を取ること。なお、バックアップの目的以外で秘密鍵の複製はできない。

秘密鍵を含む証明書のバックアップ(保存)は適宜行うことができる。秘密鍵を含む証明書のバックアップファイルは、復旧目的以外でインストールすることはできない。ただし、バックアップの目的以外で秘密鍵を含む証明書の複製はできない。

（４）各種届出に対する責任

秘密鍵の紛失、暴露、その他の危殆化又はそれらが疑われる時には、本CP/CPSに基づき速やかに届け出ること。

証明書情報に変更があった場合は、本CP/CPSに基づき速やかに届け出ること。

（５）運用規程等の遵守責任

本 CP/CPS 等を遵守すること。

9．6．3　検証者の責務

本 CP/CPS に基づき、検証者は以下の責任を果たすものとする。

（１）証明書の有効性確認責任

証明書を利用する際は、その有効性を確認すること。

（２）運用規程等の遵守責任

本 CP/CPS 等を遵守すること。

9．6．4　サービス提供者の責務

本 CP/CPS に基づき、サービス提供者は以下の責任を果たすものとする。

（１）証明書発行依頼内容に対する責任

証明書発行依頼を行う場合、本認証局に提示する依頼内容が虚偽なく正確であることに対する責任を負うこと。

（２）証明書記載事項に対する責任

証明書の記載内容について証明書受領時に内容の確認を行い、依頼内容と相違ないことを確認すること。記載内容に誤りがある場合は、速やかに当該証明書の失効手続きを行うこと。

（３）秘密鍵等の管理責任

秘密鍵を保護し、紛失、暴露、改ざん又は盗用されることを防止するために適切な措置を取ること。なお、バックアップの目的以外で秘密鍵の複製はできない。

秘密鍵を含む証明書のバックアップ(保存)は適宜行うことができる。秘密鍵を含む証明書のバックアップファイルは、復旧目的以外でインストールすることはできない。ただし、バックアップの目的以外で秘密鍵を含む証明書の複製はできない。

（４）各種届出に対する責任

秘密鍵の紛失、暴露、その他の危殆化又はそれらが疑われる時には、本CP/CPSに基づき速やかに届け出ること。

証明書情報に変更があった場合は、本CP/CPSに基づき速やかに届け出ること。

（５）運用規程等の遵守責任

本 CP/CPS 等を遵守すること。

9．6．5　その他の関係者の責務

本認証局にその他の関係者は存在しないため規定しない。

9．7　免責事項

本認証局は、認証局の責務に規定する項目に対して、本認証局の運用に携わる者が故意により損害を発生させた場合を除き、一切の責任を負わない。

9．8　補償

本認証局の責による損害が発生した場合、本認証局は、その損害に応じて補償を行う。

また、加入者、サービス提供者及び検証者がその義務を怠り、本認証局に損害を与えた場合、本認証局に対して補償を行うこととする。

9．9　補償の範囲

補償の対象は、本認証局の証明書発行対象者に限ることとし、補償については、証明書の発行又は更新にかかる費用を上限とする。
その他の第三者において生じた損害について、本認証局は一切の責任を負わない。

9．10　運用規程の有効期間と終了

本節は、本 CP/CPS の有効期間について記述する。

9．10．1　有効期間

本 CP/CPS の有効期間は、本認証局運営委員会により承認された期日以降で指定した日から、本 CP/CPS の改定までとする。

9．10．2　終了

本 CP/CPS は、本認証局が廃止となる時点で終了とする。

9．10．3　終了の影響

本 CP/CPS が終了した場合であっても、本認証局に関する責務及び権利は存続する。

9．11　関係者間の通知と連絡

本認証局から加入者及びサービス提供者への通知方法は、個別に文書の送付又は電話で連絡を行う。

9．12　改定

本節は、本 CP/CPS の改定に関する手続きについて記述する。

9．12．1　改定手続

本 CP/CPS の改定は、本認証局運営委員会において改定事項の協議を行った後、社会保険診療報酬支払基金及び国民健康保険中央会の承認の上、行う。

9．12．2　通知方法と期間

本 CP/CPS が改定された場合、速やかに証明書発行対象者に通知を行う。

9．12．3　オブジェクト識別子の変更理由

本認証局は、オブジェクト識別子を付与しないため、変更は行わない。

9．13　紛争解決手続

本認証局と証明書発行対象者との間で紛争が発生した場合、東京地方裁判所を第一審専属管轄裁判所とする。
証明書発行対象者間の紛争については、当事者間で協議して決定するものとす

る。

9．14　準拠法

本 CP/CPS に基づく認証業務から生じる紛争については、日本国の法令を適用する。

9．15　法令遵守

本認証局の関係者は、日本国内法規を遵守する。

9．16　雑則

本節は、本 CP/CPS のその他の事項について記述する。

9．16．1　完全合意条項

本認証局は、日本国内法規に則り判断を行う。

9．16．2　権利義務の譲渡

証明書発行対象者は、本 CP/CPS に定める権利又は義務を他者へ譲渡することはできない。

9．16．3　分離条項

本認証局は、日本国内法規に則り判断を行う。

9．16．4　強制執行条件

本認証局は、日本国内法規に則り判断を行う。

9．16．5　不可抗力

標準的な注意義務を尽くしても、予防・回避できない天災・事変及びシステム障害等は不可抗力とする。

9．17　その他の条項

本認証局が別の組織と合併、若しくは別の組織に移管又は譲渡する場合、新しい組織は本 CP/CPS に同意し、責任を持ち続けるものとする。

9．18　附則

この規程は、令和元年 12 月 27 日から適用する。
この規程は、令和 2 年 6 月 12 日から適用する。
この規程は、令和 2 年 9 月 24 日から適用する。
この規程は、令和 4 年 9 月 22 日から適用する。
この規程は、令和 5 年 3 月 17 日から適用する。
この規程は、令和 5 年 10 月 1 日から適用する。
この規程は、令和 5 年 11 月 22 日から適用する。

この規程は、令和 5 年 12 月 19 日から適用する。

この規程は、令和 6 年 4 月 16 日から適用する。

この規程は、令和 6 年 10 月 1 日から適用する。

この規程は、令和 7 年 2 月 19 日から適用する。

この規程は、令和 7 年 8 月 7 日から適用する。ただし、改正後の「1．5．2 問合せ先」は令和 7 年 4 月 1 日から、「1．4．3 証明書の用途」の「表 1．サーバ証明書を利用できるシステム及びサービス提供者」の電子処方箋管理サービスの追加は令和 4 年 5 月 1 日から、電子カルテ情報共有サービスの追加は令和 6 年 5 月 1 日より適用する。

この規程は、令和 8 年 4 月 1 日から適用する。