厚生労働省

医療等分野のネットワーク接続の機関認証に関する調査・研究

最終報告書

平成 30 年 3 月 30 日

ジャパンネット株式会社

目次

添付資料

■参考文献一覧

■参照規格一覧

■用語集

■別冊

1. 機関認証主体（4 文書素案）
    ① 機関認証の証明書ポリシ（CP）
    ② 認証局運用規程（CPS）
    ③ 準拠性審査基準
    ④ 事務取扱要領
2. 接続機関（2 文書素案）
    ① 接続規定
    ② セキュリティ規定
3. ネットワーク事業者（3 文書素案）
    ① 接続規定
    ② 接続認定要件
    ③ 運用ガイドライン

1. 調査概要

1.1. 背景と目的

世界に先駆けて超高齢社会に直面する我が国において、健康寿命の延伸や社会保障制度の持続可能性の確保に向けた実効的な施策の実施が急務とされている。その解決のための重要な糸口として ICT インフラの整備を通じたデータの利活用の推進が不可欠として、厚生労働省では「データヘルス改革推進本部」を立ち上げて、医療・介護のデータの有機的な連結に向けた「ICT インフラの抜本改革」や、「ゲノム解析や AI 等の最先端技術の医療への導入」の具体化を始めている。

このなかで、「全国的なネットワーク構築による医療・介護現場での健康・医療・介護の最適提供」がサービスとして検討されており、平成 29 年 6 月 9 日に閣議決定された「未来投資戦略 2017―Society 5.0 の実現に向けた改革」（以下、未来投資戦略）において、自らの生涯にわたる医療等の情報を本人が経年的に把握でき、個人・患者本位で最適な健康管理・診療・ケアを提供するための基盤として「全国保健医療情報ネットワーク」を整備するとされている。

個人・患者本位で最適な健康管理・診療・ケアを提供するにあたっては、医療機関や薬局、介護事業者、地域医療情報連携ネットワークの事業主体、更には医療情報共有サービスを提供する民間事業者等、様々な組織が全国保健医療情報ネットワークに接続してサービス提供を行う（以下、接続機関）ことが想定されるが、安心したサービス提供が行われる上でこれらの組織の信頼性を確認するための認証（以下、機関認証）が必要となる。

そこで、本事業は全国保健医療情報ネットワークが整備されることを前提として、全国保健医療情報ネットワークに接続する機関の認定基準や認証方法、認証主体の具体化やセキュリティポリシーについて調査研究を実施し、平成 30 年度以降の全国保健医療情報ネットワークの要件検討を実施する際の検討材料を提供することを目的として機関認証に係る調査研究を実施した。

1.2. 検討の前提

1.2.1. 機関認証の必要性について

全国保健医療情報ネットワークへの接続するための機関認証を受けるにあたっては一定の安全基準を満たしていることが求められるが、医療等サービス提供側から見た場合、必ずしもすべての機関や利用シーン（ユースケース）において機関認証が必要とされない可能性がある。

本事業においては、全国保健医療情報ネットワーク側から見た場合、接続機関を認証することを前提にその認定基準や認証方法を検討し、機関認証が対象とすべき接続機関の範囲やユースケースについては検討対象としていない。

1.2.2. 他の検討との関係

本事業の実施にあたり、これまでに機関認証や相互接続基盤について調査研究された 2 つの事業の検討内容を特に参考にした。

（１）厚生労働省事業

厚生労働省「平成 28 年度　医療情報連携ネットワークにおける標準規格準拠性の検証機関の実現に向けた調査研究業務」（以下、平成 28 年度調査研究）において、全国の地域医療情報連携ネットワーク同士の接続による地域間連携を支援する組織として地域間連携サポートセンタが検討され、その機能の一つとして地域医療情報連携ネットワークの事業主体に対して組織用証明書を発行する組織認証の在り方が検討されている。本事業では平成 28 年度調査研究の組織認証に関する検討内容を踏まえて、機関認証主体に関する調査研究を実施した。本報告書の「機関認証」は平成 28 年度調査研究の「組織認証」と同義として検討を行った。

（２）総務省実証事業

医療等分野においては用途別・地域別にネットワークが構築されているため、今後見込まれるオンライン資格確認やオンライン請求、地域医療情報連携ネットワーク同士の連携、医療介護連携、電子紹介状、電子処方箋、高精細映像伝送等様々なサービスの普及にあたりネットワーク同士の相互接続が必要になる。そこで、総務省は「平成 28 年度補正予算　医療等分野における高精細映像等データ共有基盤の在り方に関する実証」（以下、総務省実証）において、医療等分野の各種サービスに共通利用可能な公的広域ネットワークに向けた医療等分野のデータ共有基盤（以下、相互接続基盤）の実用化にあたり、必要となる技術運用課題の抽出を目的に実証を行っている。

総務省実証において、相互接続基盤で必要となる機能の一つとして機関認証が検討されていることや相互接続基盤の運用に資する各種規定類の作成が行われていることから、総務省実証の検討内容についても参考にして検討を行った。

1.2.3. 他の機関認証主体の調査

本事業の実施にあたり、機関認証を実施している既存の認証局であるオンライン請求システム専用認証局について、「オンライン請求システム専用認証局　運用規程」（以下、参考文献(1)）[1]を調査した。機関認証主体について検討するにあたり、機関の審査方法や証明書記載情報、証明書配付方法、証明書代金等参考にした。

[1] 本報告書で言及する参考文献については巻末の「参考文献一覧」を参照。

（１）証明書の用途

参考文献(1)の「第１　概説」「４　証明書の用途」に以下の通り記述されている。

- オンライン請求システムを利用する際の認証及び暗号化通信
- オンライン請求システムにおいて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

（２）証明書の発行対象

参考文献(1)の「第１　概説」「３　関係者」「(2)　証明書発行対象者」「ア　加入者」に以下の通り記述されている。

- 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
- 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
- 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
- 高齢者の医療の確保に関する病院または診療所その他適当と認められるもの（特定健診健康診査実施期間、特定保健指導実施期間）
- 労働者災害補償保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もしくは診療所または都道府県労働局長の指定する病院もしくは診療所、薬局（労災指定医療機関等）
- 商業登記簿の写しで確認可能なレセプトコンピュータ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）
- 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）

（３）識別名に関する命名規則

参考文献(1)の「第３　識別及び認証」「１　識別名」「(2)　識別名に関する要件」に記述されている。図表 1-1 に抜粋を示す。

図表 1-1　識別名に関する命名規則（抜粋）

証明書対象	項目	記載内容
保険医療機関、保険薬局、労災指定医療機関等、請求事務代行等	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）	組織の識別子として、医科（medical）、歯科（dental）または調剤（pharmacy）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また

証明書対象	項目	記載内容
		は薬局コード（7 桁）を連結した 10 桁固定のコードまたは事務代行者コード（10 桁固定）を記載する。
保険者	組織単位名（Organizational Unit）	組織の識別子として、保険者（insurance）を記載する。
	一般名（Common Name）	保険者番号（8 件固定）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）	組織の識別子として、kenshin 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、特定健診・特定保健指導機関コード（10 桁）を記載する。
システムベンダ・販売会社	組織単位名（Organizational Unit）	組織の識別子として、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）または保守用証明書（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。

（４）機関等の審査

参考文献(1)の「第３　識別及び認証」「２　新規の証明書発行時の本人性確認」「(2)機関等の審査」に、証明書発行時の本人性確認方法について以下の通り記述されている。

- 加入者から証明書の発行依頼を受領した場合は、依頼を行った機関等が適切かを社会保険診察報酬支払基金が所有する情報と依頼書との検証により審査を行う。
- 加入者がシステムベンダ・販売会社である場合は、商業登記簿の写し及び社会保険診察報酬支払基金が所有する情報と依頼書との検証により審査を行

う。

また「第３　識別及び認証」「３　証明書更新時の本人性確認」「４　証明書更新時の本人性確認」に、証明書発行時や失効時の本人性確認方法について以下の通り記述されている。

- 有効期間終了の場合、社会保険診察報酬支払基金が所有する情報を基に証明書の記載内容の変更の有無を確認し、変更がない場合は本人性確認が完了しているものとする。変更がある場合は、更新は行わず、新規発行同様の取扱いとする。
- 証明書失効の場合は、証明書の更新は行わず、新規発行時と同様の取扱いとする。
- 証明書を失効する際の認証については、新規発行時と同様の取扱いとする。

（５）オフラインでの証明書配付方法

参考文献(1)の「第４　証明書のライフサイクル」「３　証明書の発行」「(2)　証明書発行の通知」に、システムベンダ・販売会社やサービス提供者への配付方法について以下の通り記述されている。

- システムベンダ・販売会社に対して証明書を発行した場合、証明書を格納した電子媒体、証明書の復号化のためのパスワード及び本認証局の自己署名証明書を、配達状況を確認できる方法（書留等）で送付、もしくは手交する。
- サービス提供者に対して証明書を発行した場合、証明書を格納した電子媒体を手交する。

（６）利用者証明書の有効期間

参考文献(1)の「第６　技術的セキュリティ」「３　鍵ペア管理に関するその他の留意事項」「(2)　公開鍵証明書の有効期間及び鍵ペアの使用期間」に、利用者証明書の有効期間について以下の通り記述されている。

- 保険医療機関、保険薬局、保険者、特定健康診査実施機関、特定保健指導実施機関、労災指定医療機関等及び請求事務代行者
  証明書有効期間：初回３年２ヶ月、更新時３年３ヵ月
- システムベンダ・販売会社
  証明書有効期間：１年１ヶ月

（７）監査

参考文献(1)の「第８　監査」に図表 1-2 の通り記述されている。

図表 1-2　監査内容

#	実施項目	説明
1	監査頻度	監査は、1 年に 1 度の頻度で定期監査を行う。
2	監査者の身元・資格	監査人は、十分な知識を持ったものが行う。
3	監査者と被監査者の関係	監査人は、本認証局運営要員以外から選定する。
4	監査の項目	監査では、認証業務が本規程の基準及び手順に則って実施されていること並びに不正行為等の対策が機能していることを検証する。
5	監査指摘事項への対応	認証局責任者の指示のもと、監査における指摘事項に対する改善措置を行う。
6	監査結果の通知	監査人は、監査結果について監査報告書を作成し認証局責任者へ報告する。

（８）証明書の発行代金

社会保険診察報酬支払基金ホームページ[2]の「保険医療機関・保険薬局に係るオンライン請求」「4.　オンライン請求の手続きについて」「(2) セキュリティ関係」「イ　電子証明書の取得」に以下の通り記述されている。

- 発行事務コスト：4,000 円

1.3. 本事業の概要

1.3.1. 実施内容

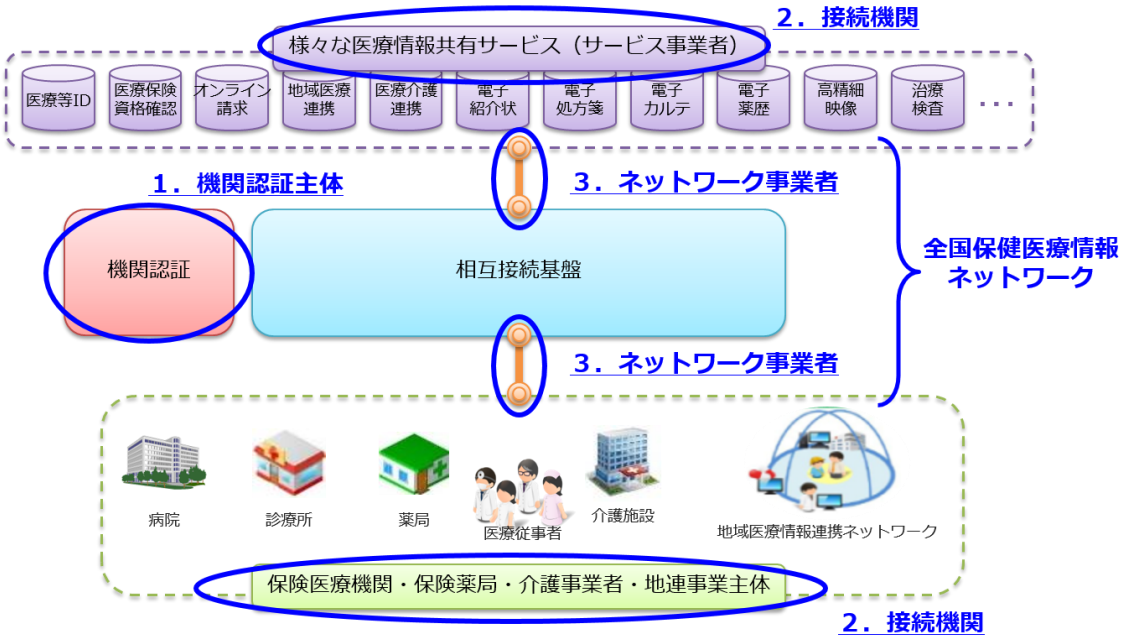
本事業は図表 1-3 で示す「1. 機関認証主体」、「2. ネットワーク事業者」、「3. 接続機関」を対象として、図表 1-4 に示した内容を実施した。なお、「3. 接続機関」としては以下の 5 種類を想定した。

1) 保険医療機関
2) 保険薬局
3) 地域医療情報連携ネットワークの事業主体（以下、地連事業主体）
4) 介護保険法における介護事業者（以下、介護事業者）
5) 医療情報共有サービスを提供する民間事業者（以下、サービス事業者）

上記以外で行政機関や情報収集機関等も接続機関として考えられるが、本事業では対象外とする。

[2]ホームページは、
（http://www.ssk.or.jp/seikyushiharai/online/iryokikan/index.html）を指す。

図表 1-3　調査研究対象[3]



図表 1-4　調査研究内容

#	テーマ	対象	内容
1	全国保健医療情報ネットワークに接続する機関認証主体の調査研究	機関認証主体	全国保健医療情報ネットワークに接続する機関を認証するための認証スキームについての調査研究を実施した
2	全国保健医療情報ネットワークに接続する機関認証方式の調査研究	機関認証主体、接続機関	全国保健医療情報ネットワークに接続する機関について想定し、認証する方法について調査研究を実施した
3	ネットワーク事業者の接続規定の調査研究	ネットワーク事業者	ネットワーク事業者が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式、接続認定のためのセキュリティ基準、運用要件について調査研究を実施した
4	接続規定、ガイドラインの策定に向けた調査研究及び素案の作成	機関認証主体、接続機関、ネットワーク事業者	上記 1～3 で調査研究を実施した内容を基に証明書ポリシや認証局の要件、認証局の運用規程、接続のセキ

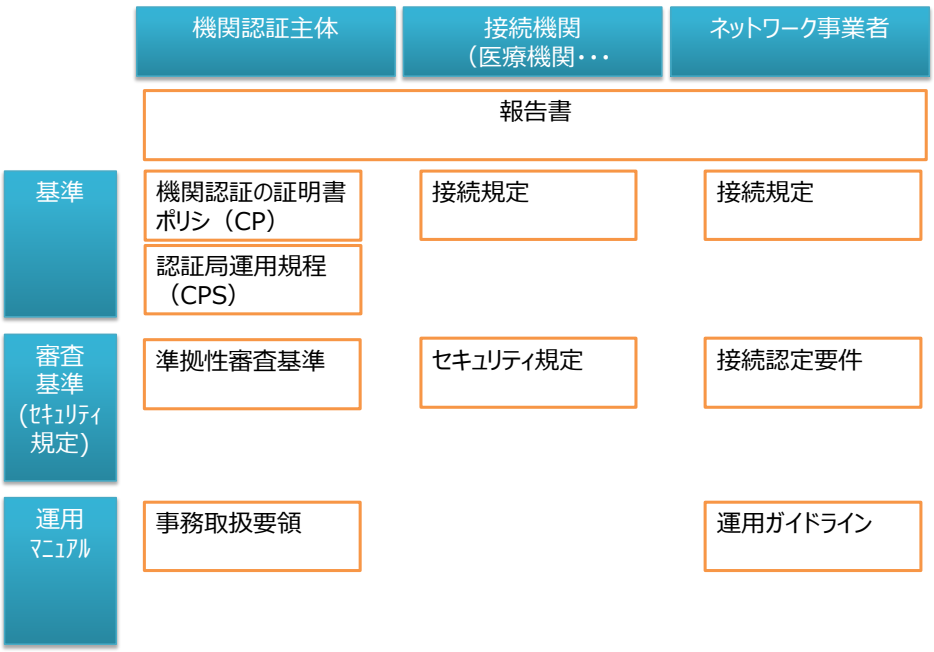
[3]出典：未来投資会議構造改革徹底推進会合「健康・医療・介護」会合（第２回）
厚生労働省・総務省・経済産業省　提出資料「（２）データ利活用基盤の構築」を参考に作成。

#	テーマ	対象	内容
			ュリティポリシーの必要な技術文書について、素案を策定した
5	コスト試算	機関認証主体、接続機関、ネットワーク事業者	上記１～４で調査研究を実施した内容を基に機関認証の認定、認証にかかるイニシャルコスト、運用コストを試算した
6	接続検証	機関認証主体、接続機関、ネットワーク事業者	策定した準拠性審査基準に適合する環境において検証用証明書を発行し、ネットワークレベルの機関認証用について接続検証を実施した。アプリケーションレベルの機関認証用証明書については TLS1.2 高セキュリティ型のクライアント認証（サーバ認証を含む）の接続検証を実施した

本事業の成果は、調査研究報告書並びに調査研究結果をもとに、機関認証主体、ネットワーク事業者、接続機関に関して作成する以下の規定類の素案である（図表 1-5）。

- 機関認証主体（4 文書）
  - 機関認証の証明書ポリシ（CP）
  - 認証局運用規程（CPS）
  - 準拠性審査基準
  - 事務取扱要領
- 接続機関（2 文書）
  - 接続規定
  - セキュリティ規定
- ネットワーク事業者（3 文書）:
  - 接続規定
  - 接続認定要件
  - 運用ガイドライン

図表 1-5　本事業の成果ドキュメント

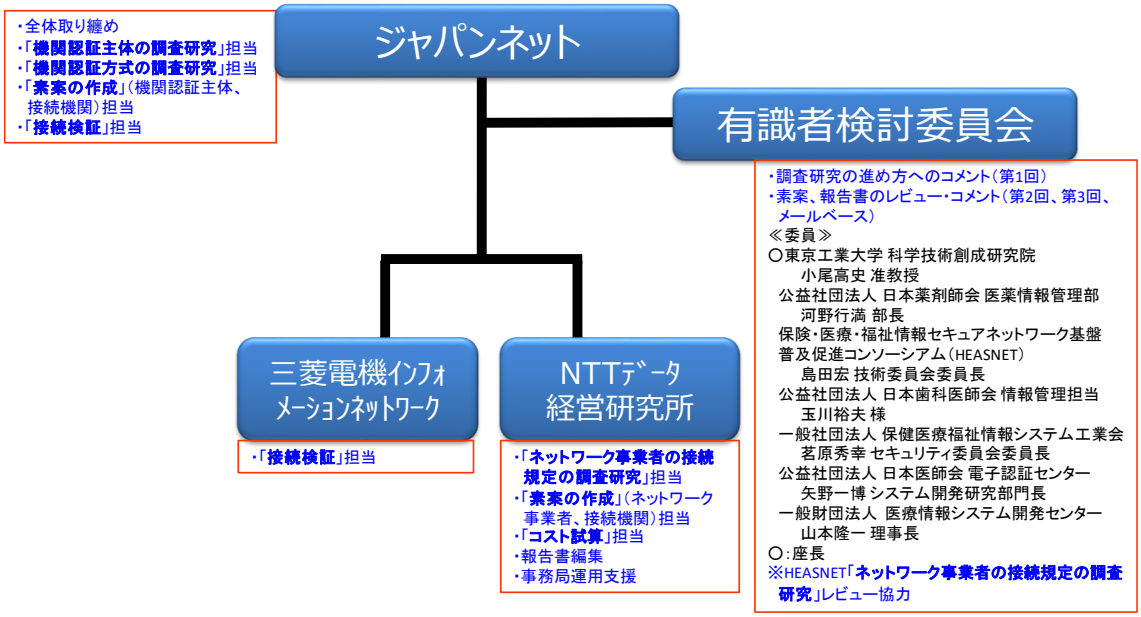


1.3.2. 実施体制

本事業は図表 1-6 で示す通り、ジャパンネット株式会社（以下、JN）が受託し、ネットワーク事業者の接続規定の調査研究ならびに素案の策定、コスト試算に株式会社 NTT データ経営研究所（以下、NDK）、接続検証に三菱電機インフォーメーションネットワーク株式会社（以下、MIND）が参画した。

また、認証局、保健医療福祉分野の公開鍵基盤（以下、HPKI）、ネットワークセキュリティに関する知識・知見がある有識者で構成される「有識者検討委員会」（以下、検討委員会）を設け、事務局案に対する検討やドキュメントレビューを実施した。

図表 1-6　実施体制



検討の具体化にあたっては、調査研究テーマごとに有識者に別途協力を依頼して実施した。

機関認証主体並びに機関認証方式の調査研究については、認証局の運営経験や運営に向けて検討を進めている機関として日本医師会、日本薬剤師会、日本歯科医師会、一般財団法人 医療情報システム開発センター（以下、MEDIS）、HPKI 技術に関する標準化活動を推進している一般社団法人 保健医療福祉情報システム工業会（以下、JAHIS）に別途、検討やレビュー協力を依頼し、具体的な検討を行った。

ネットワーク事業者の接続規定の調査研究については、ネットワーク事業者の立場からの検討を行うため、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム（以下、HEASNET）参加企業 5 社に協力を依頼し、具体的な検討を行った。

1.3.3. 実施スケジュール

本事業は図表 1-7 で示すスケジュールで実施した。平成 29 年 12 月 25 日に第 1 回検討委員会を実施し、本事業において検討すべき課題について議論し、今後の検討具体化に向けた協力要請を行った。1 月末まで各調査研究テーマについて調査研究を行い、2 月末を目途に報告書骨子や規程類の素案を作成した。第 2 回検討委員会での中間レビュー、第 3 回検討委員会での最終レビューを経て、報告書や規程類の素案を 3 月末までにまとめた。

図表 1-7　実施スケジュール

実施内容	担当	支援	12 月	1 月	2 月	3 月
有識者検討委員会	JN、NDK	有識者検討委員会		△第 1 回（12/25）	△第 2 回（2/20）	△第 3 回（3/13）
1.調査研究 1)機関認証主体 2)機関認証方式 3) ネットワーク事業者の接続規定	JN、NDK	有識者検討委員会、HEASNET 参加企業	・資料収集、目次案	・調査研究	・報告書骨子作成	・最終報告書作成
				・HPKI、認証局関連ヒアリング（1/22～2/14） 日本薬剤師会（1/22） 日本医師会（1/23） JAHIS（1/24） MEDIS（1/25） 日本歯科医師会（2/14）		
				・審査関連ヒアリング（1/29～1/31） 1 指定都市（1/29） 1 県（1/31）		
					△機関認証関連 有識者検討委員会事前会議（2/9）	
					・ネットワーク事業者規定レビュー（2/7～3/8） HEASNET（2/7、3/5、3/8）	
2.接続規定・ガイドラインの素案作成	JN、NDK	HEASNET 参加企業		・資料収集、目次案	・素案作成	・素案まとめ
3.コスト試算	JN、NDK			・資料収集、目次案	・調査研究	・最終報告書作成
4.接続検証	JN、MIND				・接続環境構築	・接続検証 ・最終報告書作成
マイルストン				△中間報告書（12/28）	△素案機関認証主体（2/15） △報告書骨子 △素案接続機関、ネットワーク事業者（2/28）	△最終報告書（3/30）

2. 全国保健医療情報ネットワークに接続する機関認証主体

全国保健医療情報ネットワークに接続する機関を認証するための認証スキームについての調査研究を実施した。

2.1. 認証の主体のあり方

2.1.1. 事業主体

保健医療福祉分野で機関認証用証明書を発行する機関認証主体については、厚生労働省の「保健医療福祉分野 PKI 認証局認証用（組織）証明書ポリシ 1.1 版」（以下、HPKI-CP。参考文献(2)）が存在しているが、「厚生労働省　平成 28 年度　医療情報連携ネットワークにおける標準規格準拠性の検証機関の実現に向けた調査研究業務 別冊報告書『地域間連携を円滑に行うための方策と必要な機能要件にかかる検討』」（以下、参考文献(3)）において、発行対象を保険医療機関、保険薬局から地連事業主体とした場合の要件として、HPKI-CP がベースとする ISO17090（参照規格(1)）に準拠することを要件としている。

接続機関が多岐にわたることを前提とする本事業においても ISO17090 を要件とし、接続機関が厚生労働省の「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以下、HPKI 認証局専門家会議）による監査（以下、準拠性監査）を受けることを想定した。

過去の検討（参考文献(3)）においては、機関認証主体は①公益性を担保できること、②ガバナンスを発揮できること、③保健医療福祉分野における関係団体と綿密な連携ができること、④全体最適化を可能とすること、という要件が必要になると考えられること、また、社会インフラとしての公益性や全体最適性を担保するため、公的組織が事業主体となることが望ましいとされた。しかし、HPKI 認証局専門家会議の準拠性監査を受けるのであれば、公的組織である必要はないと考えられる。

一方、営利企業による運営を否定するものではないが、とりわけ全国保健医療情報ネットワークの立ち上げ段階においては非営利組織であることが望ましい。非営利組織としては、公益社団法人や一般社団法人、一般財団法人等が想定される。

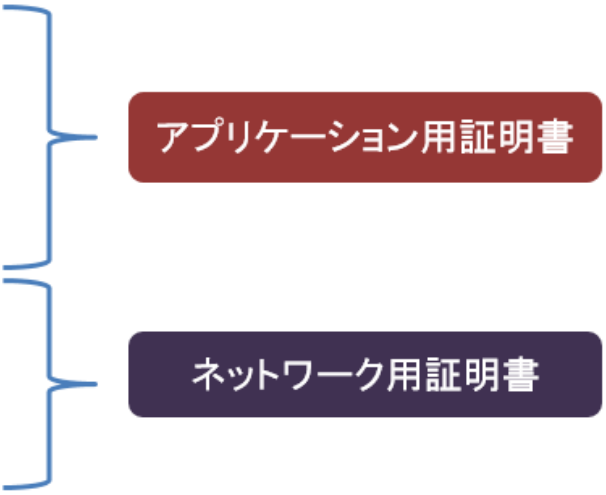
したがって、公共性が担保され事業継続性を確保した第三者機関が HPKI 認証局専門家会議の準拠性監査を受けて運営することが相応しいと考える。

2.1.2. 機関認証用証明書の種類

機関認証を OSI 7 階層モデルで示される 1～3 層に相当するネットワーク層までの認証を行うか、4 層以上のアプリケーション層の認証を行うか検討を行った（以下、ネットワークレベル、アプリケーションレベル）。

図表 2-1　OSI 7 階層モデルと利用される証明書の関係

階層番号	名称	規定している内容
7	アプリケーション層 (Application Layer)	業務に依存した処理
6	プレゼンテーション層 (Presentation Layer)	データ表現方法の取り決め (使用する文字コードなど)
5	セッション層 (Session Layer)	業務を開始／終了するための取り決め
4	トランスポート層 (Transport Layer)	アプリケーション同士の電文の送受信
3	ネットワーク層 (Network Layer)	コンピュータ同士の電文の送受信
2	データリンク層 (Data Link Layer)	隣接したノードに1ビットを転送する
1	物理層 (Physical Layer)	伝送路の物理特性(ハードウェア依存)



ネットワークレベルについてはネットワーク事業者が独自に電子証明書を発行しているケースがあるため主にアプリケーションレベルの用途を想定して検討を行い、ネットワークレベルにおいて使用することも可能にしておくことでネットワーク事業者の選択に委ねる考えができる。

一方、確実に医療機関を認定するならばネットワークレベルにおいて認証すべきであるが、その場合、全国で膨大な数の医療機関の認証が必要となるためデレゲーション（機関に対する審査業務の外部への委任）を行う等の運用上の工夫が必須である。

ネットワークレベルにおいてもアプリケーションレベルにおいても機関認証主体としての接続機関の認定ルール自体に変わりはないと考えられる。そのため、機関認証主体は、ネットワークレベルとアプリケーションレベルのいずれにおいても、医療機関等を確実に確認できるような証明書を発行すると仮定し、発行する証明書の種類は、ネットワークレベルの機関認証用証明書とアプリケーションレベルの機関認証用証明書の 2 種類と想定して検討を行った。

2.1.3. 機関認証主体の役割

機関認証用証明書の必要性は全国保健医療情報ネットワーク上で提供されるサービスの求める認証レベルによるため、ネットワークレベルとアプリケーションレベルのいずれの機関認証用証明書も全国保健医療情報ネットワークを利用するために必須ではないと考えられる。しかし将来的に機関認証用証明書を必須とするサービスが始まることを想定し、発行する証明書は全国保健医療情報ネットワークへの接続やその上で提供されるサービスで利用可能な認証レベル（機関の実在性や資格、所在地からの要求の証明）を満たすものとする。このため機関認証主体は接続機関の実在性や申請意思、有資格性を確認した上で、証明書を発行する。接続機関からの申請を正確に審査し、その機関の所在地へ確実に証明書を配付することが重要である。

さらに本事業では、接続機関が全国保健医療情報ネットワークに接続するために機関認証主体が審査する際のセキュリティ基準を検討し、「セキュリティ規定」の素案を作成した。このため機関認証主体は接続機関の実在性や申請意思、有資格性に加え、セキュリティ要件を満たすことの確認を実施する。

機関認証主体が上記 2 つの役割を果たす結果、機関認証用証明書を発行された接続機関は、その機関自体と利用環境が全国保健医療情報ネットワークを利用可能であると判断できると考えられる。このことから、相互接続基盤側との協議が必要となるが、機関認証主体は接続機関が全国保健医療情報ネットワークを利用するための審査機関の役割を担い、機関認証用証明書が全国保健医療情報ネットワークを利用するための認定証とすることが考えられる。

2.1.4. 厚生労働省ルート認証局との接続

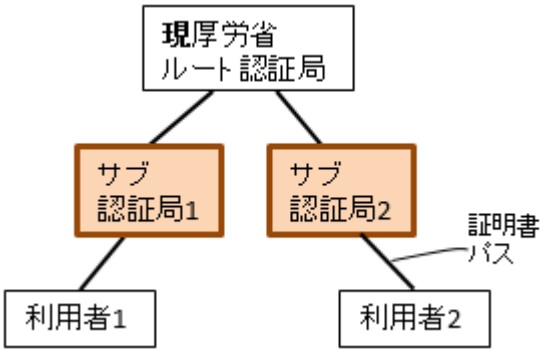
HPKI 認証用（人）認証局（以下、人認証用認証局）においては、厚生労働省ルート認証局との接続が必須とされている。HPKI 認証用（組織）認証局（以下、機関認証用認証局）においても厚生労働省ルート認証局との接続が必要か検討する必要がある。

（１）現厚生労働省ルート認証局と接続する場合

機関認証用認証局が人認証用認証局と同様の管理の証明書ポリシとすると、厚生労働省ルート認証局と接続することが相応しく思われる。認証局は図表 2-2 の構成となる。

しかし人認証用証明書と同じ信頼点となり、既に人認証用証明書をクライアント認証に用いているサービスでは、単純な TLS クライアント認証だけであればクライアント証明書のルート証明書がサーバに信頼点登録されているかの確認であるため、機関認証用証明書でも接続できてしまう懸念があり、現行の厚生労働省ルート認証局との接続は望ましくないと考えられる。

図表 2-2　現厚生労働省ルート認証局接続サブ認証局構成

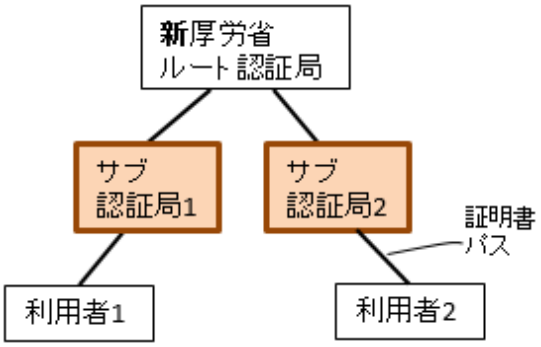


（２）新厚生労働省ルート認証局と接続する場合

現行の厚生労働省ルート認証局でなく、機関認証用に新規の厚生労働省ルート認証局を構築して接続する可能性が考えられる。新たな信頼点となり、機関認証専用の認証が実現できる。認証局は図表 2-3 の構成となる。

接続機関として地連事業主体、サービス事業者といった厚生労働省の所管業務以外の事業者にも機関認証用証明書が発行されることになる。 HPKI-CP に則っているとはいえ、保健医療福祉分野以外の機関に証明書を発行する認証局が厚生労働省ルート認証局と接続することは望ましくないと考えられる。

図表 2-3　新厚生労働省ルート認証局接続サブ認証局構成

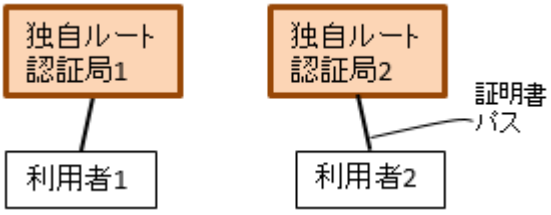


（３）厚生労働省ルート認証局と接続しない場合(1) - 複数独自ルート認証局構成 -

厚生労働省ルート認証局と接続しなくても、ISO 17090 に準拠した独自のルート認証局として HPKI 認証局専門家会議の準拠性監査を受けることで、厚生労働省のガバナンスを効かせることができる。認証局は図表 2-4 の構成となる。

ただし厚生労働省ルート認証局と接続しない場合、各機関認証用認証局がルート認証局となり各々の相互認証や証明書の検証者側で複数のルート認証局の証明書を信頼点として管理する等の手間が必要になる点に留意が必要である。

図表 2-4　複数独自ルート認証局構成



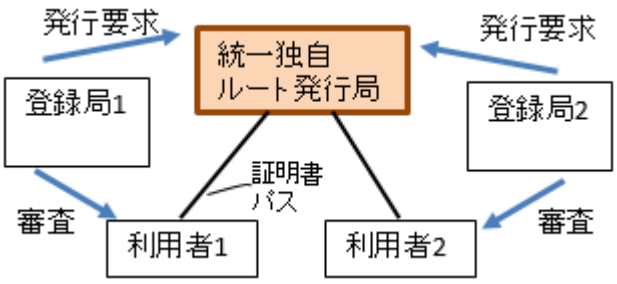
（４）厚生労働省ルート認証局と接続しない場合(2) - 統一独自ルート発行局＋複数登録局構成 -

相互認証や信頼点管理の手間を減らすため、ルート認証局を増やさない方法とし

て、証明書発行を行う発行局を統一する構成が考えられる。認証局は図表 2-5 の構成となる。

ただし全ての登録局が統一ルート認証局を利用するとは限らないことや、証明書の検証側が複数のルート認証局の証明書を信頼点として認める場合がある点に留意が必要である。

図表 2-5　統一独自ルート発行局＋複数登録局構成



（５）厚生労働省ルート認証局との接続の要否

（１）、（２）の検討結果から厚生労働省ルート認証局との接続は不要と考える。また（３）、（４）で検討した独自にルート認証局となる場合の構成については、証明書の検証側となる医療情報ネットワークの運営主体や医療情報ネットワーク上で提供されるサービスの認証ポリシによるため、構成については、特定していない。

2.2. 認証主体の業務

機関認証主体の業務は、図表 2-6 に示す内容が考えられる。

図表 2-6　機関認証主体の業務

#	想定業務	概要
1	接続機関からの発行申請等受付	接続機関からの申請受付
2	接続機関の組織の正当性審査	接続機関の審査
3	機関認証用証明書の発行と配付	機関認証用証明書の発行と機関認証用証明書の配付
4	機関認証用証明書の失効	接続機関からの申請に基づく失効 機関認証用認証局による失効 失効リスト（Certificate Revocation List：CRL）の公開
5	機関認証用証明書の更新（継続）	機関認証用証明書有効期限切れに伴う、接続機関からの申請に基づく機関認証用証明書の更新（継続）

#	想定業務	概要
		有効期限切れにともなう接続機関への有効期限切れ通知
6	機関認証用証明書の再発行	接続機関の組織の変更等における再審査、再発行等の管理
7	審査結果の管理	審査結果の保管・管理
8	機関認証用証明書に関する問い合わせ対応	接続機関等からの機関認証用証明書に関する問い合わせ対応
9	審査基準の策定	認証局運用規程（CPS)の策定と公表
10	テスト用証明書の発行と配付	接続機関へのテスト用証明書の発行と配付
11	機関認証用証明書情報の公開	機関認証用証明書検証者の確認用 機関認証用証明書取得組織自身の証明書情報等確認用 後述の「発行通知書」の確認用

図表 2-6 に示した業務は、通常認証局が実施すべき業務と考える。本事業では、全国保健医療情報ネットワークに接続する機関の認証方法を調査することから、認証方法と密接に関わる#1 から#6 の業務について検討し詳細化することとした。

検討した結果については、後述の「2.4 接続機関の認定基準」「3.2 発行対象別審査方法（法人、個人事業主、医療及び介護施設)」及び「3.3 機関認証用証明書ライフサイクル別審査方法（新規発行、更新発行、再発行)」で記載する。

また、検討結果を基に、本事業の作成ドキュメントである「機関認証の証明書ポリシ」「認証局運用規程」「準拠性監査基準」及び「事務取扱要領」を作成し、特に事務取扱要領にて詳細化した手順を記述している。

2.3. 接続機関の認定方法

接続機関の認定方法として、以下の 3 つの手順を定義した。

1) 審査

- 「3.2 発行対象別審査方法（法人、個人事業主、医療及び介護施設)」に基づき、接続機関の審査を実施する。

2) 証明書発行

- 審査に合格した場合、機関用の OID（「3.1 機関認証用証明書記載情報（機関用 OID、hcRole(healthcare Role))」にて後述）を採番した上、プロファイルに則った証明書を発行する。

3) 証明書配付

- 申請された所在地へ確実に届くよう、証明書を配付する。
- 別途申請者へ、機関認証用証明書の発行を受けていることを表す「発行通知

書」を送付する。「発行通知書」はネットワーク事業者に対し機関認証用証明書を所持していることを示す等、サービス事業者に対し機関認証用証明書に記載された ID 情報を通知するため等に用いることを想定する。

なお、「発行通知書」記載内容は図表 2-7 を想定した。

図表 2-7　発行通知書記載内容

#	記載内容
1	機関名
2	機関の所在地
3	機関認証用証明書の有効期間
4	機関認証用証明書の ID 情報 （証明書に記載された OID や証明書シリアル番号等を想定）

2.4. 接続機関の認定基準

本事業が想定する接続機関は前述の通り、保険医療機関、保険薬局、地連事業主体、介護事業者、サービス事業者である。

保険医療機関、保険薬局については HPKI-CP において、地連事業主体については参考文献(3)において、機関認証の認定基準について検討が行われている。そこで、介護事業者の認定基準について、保険医療機関や保険薬局の考え方を踏襲することができるか検証するため、介護事業者の指定手続及び保険医療機関・保険薬局の指定手続を文献調査及び関連組織にヒアリングを実施し、認定基準の検討を行った。また、サービス事業者の認定基準については、参考文献(3)の考え方を踏襲することができるか検討を行った。

調査の結果、詳細は「2.4.3 認定基準について」に記載するが、介護事業者、保険医療機関及び保険薬局については、各々を所管する都道府県、市町村、地方厚生局から「指定通知書」が発行されることが明らかとなり、介護事業者、保険医療機関、保険薬局の認定基準は、有効な「指定通知書」を有していることが必要と考えた。

また、サービス事業者の認定基準は、全国保健医療情報ネットワークにおいて何らか発生した事象によっては法的な責任を負う必要があり、この責任の所在を明確にするためには、法人か個人事業主である必要があると考え、参考文献(3)における地連事業主体の認定基準と同じ考えを踏襲することが必要と考えた。

ただし、実務上は保険医療機関でないケース（遠隔診療のみ実施している機関等）も考えられ、「指定通知書」を保有していない場合における認定基準は、今後の検討課題である。

2.4.1. 調査方法

文献調査により、指定通知書に基づいた認定を想定し、指定手続の詳細を把握した上で仮説の妥当性を検証するため、図表 2-8 の通りヒアリングを実施した。

図表 2-8　ヒアリング調査概要

ヒアリング対象	実施日	主なヒアリング事項
日本薬剤師会	平成 30 年 1 月 22 日	機関認証主体の業務について
日本医師会	平成 30 年 1 月 23 日	機関認証主体の業務について
JAHIS	平成 30 年 1 月 24 日	HPKI の技術面について
MEDIS	平成 30 年 1 月 25 日	機関認証主体の業務について
1 指定都市	平成 30 年 1 月 29 日	介護事業者の指定許可について
1 県	平成 30 年 1 月 31 日	介護事業者の指定許可について
日本歯科医師会	平成 30 年 2 月 14 日	保険医療機関の指定許可について

2.4.2. 調査結果

（1）保険医療機関、保険薬局の指定

保険医療機関、保険薬局の指定を受けるためには、まず医療機関・薬局の開設許可を都道府県から受ける必要がある。図表 2-9 図表 2-9 に医療機関・薬局の開設手続の概要を示す。

図表 2-9　医療機関・薬局の開設手続概要

<table>
<tr><th rowspan="2">種別</th><th rowspan="2">所管</th><th rowspan="2">申請時
必要書類</th><th rowspan="2">必要資格</th><th colspan="3">指定／許可</th></tr>
<tr><th>書類</th><th>採番番号</th><th>有効期間</th></tr>
<tr><td>医療機関</td><td rowspan="2">都道府県</td><td rowspan="2">・開設許可申請
・法人の場合
登記事項証明書

その他必要書類</td><td rowspan="2">・法人
・個人事業者</td><td>・開設許可証
・診療所開設届済証</td><td rowspan="2">都道府県独自の番号体系で採番</td><td rowspan="2">6 年

※6 年毎に更新申請が必要</td></tr>
<tr><td>薬局</td><td>・薬局開設許可証</td></tr>
</table>

開設許可を受けた医療機関・薬局が、保険医療機関・保険薬局の指定を受ける場合は、所管の地方厚生局において指定申請手続を実施する。指定されると指定通知書が交付され、医療機関番号（指定通知書では「医療機関コード」「薬局コード」）が採番される。図表 2-10 に保険療機関・保険薬局の指定手続の概要を示す。

図表 2-10　保険医療機関・保険薬局の指定手続概要

種別	所管	申請時 必要書類	必要資格	指定／許可		
				書類	採番番号	有効期間
保険医療機関 保険薬局	地方厚生局	・指定申請書 ・法人の場合 登記事項証明書 その他必要書類	・法人 ・個人事業主	指定通知書	医療機関番号 （7 桁）	6 年 ※6 年毎に更新申請が必要

（２）介護事業者の指定

介護事業者の指定を希望する事業者は、所管の都道府県または市町村に対して、指定申請を行う必要がある。指定されると指定通知書（開設許可通知書）が交付され、事業所毎に介護保険事業所番号が採番される。

なお、健康保険法の保険医療機関・保険薬局に指定された医療機関・薬局は、介護保険法による医療系サービスの事業者として、指定をされたものとみなされる。この場合、既に採番されている医療機関コード（7 桁）に、頭 3 桁付与した番号が、介護保険事業所番号となる図表 2-11、図表 2-12 に介護事業者の指定手続の概要を示す。

図表 2-11　介護事業者の指定手続概要 1

種別	所管	申請時 必要書類	必要 資格
指定居宅サービス事業者	・都道府県 ・指定都市 ・中核市	・指定申請書 ・定款、寄附行為等及びその登記簿謄本または条例等 その他必要書類	法人 ※県条例で法人ではない事業者を指定するケースも存在するが、現在はほぼない。
指定居宅介護支援事業者 （平成 30 年 4 月から市町村へ委譲）			
介護保険施設			
指定介護予防サービス事業者			
指定地域密着型サービス事業者	・市町村		
指定地域密着型介護予防サービス事業者			
指定介護予防支援事業者			
みなし指定	・都道府県 ・指定都市 ・中核市 ・市町村	必要なし	健康保険法の保険医療機関・保険薬局に指定された医療機関・薬局 法人／個人事業主

図表 2-12　介護事業者の指定手続概要 2

<table>
<tr><th rowspan="2">種別</th><th colspan="3">指定／許可</th></tr>
<tr><th>書類</th><th>採番番号</th><th>有効期間</th></tr>
<tr><td>指定居宅サービス事業者</td><td rowspan="2">・指定通知書</td><td rowspan="4">介護保険事業所番号（10 桁）

・サービス種別かつ事業所毎
・同一事業所名・同一所在地であれば特例として複数サービスを同一番号で指定可能</td><td rowspan="4">6 年

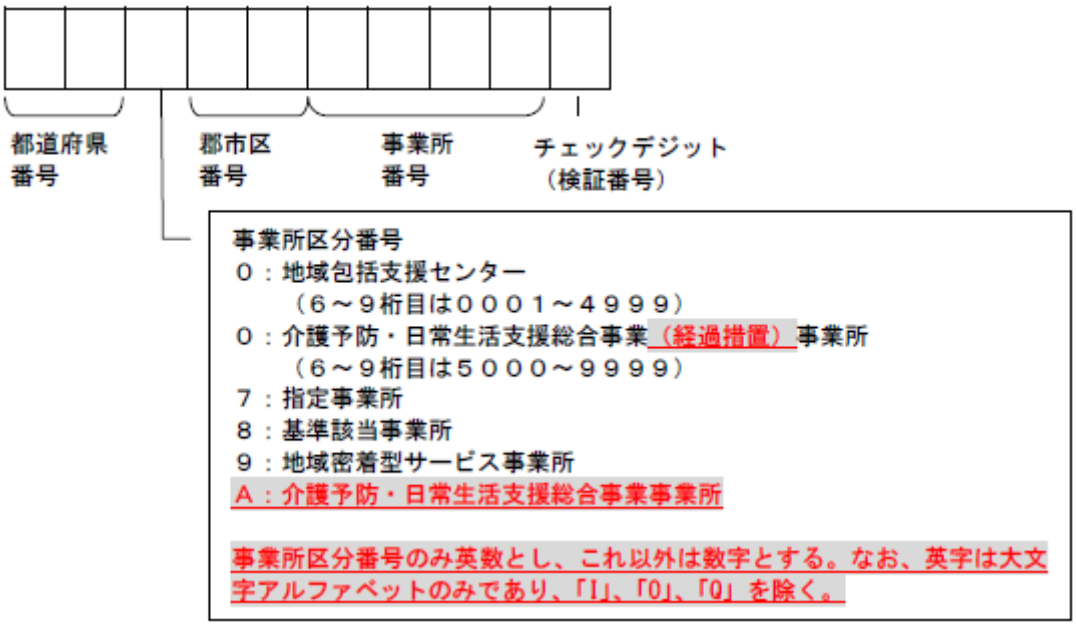
※6 年毎に更新申請が必要</td></tr>
<tr><td>指定居宅介護支援事業者
（平成 30 年 4 月から市町村へ委譲）</td></tr>
<tr><td>介護保険施設</td><td>・指定通知書
（介護老人福祉施設）
・開設許可通知書
（介護老人保健施設）</td></tr>
<tr><td>指定介護予防サービス事業者</td><td rowspan="4">・指定通知書</td></tr>
<tr><td>指定地域密着型サービス事業者</td><td></td><td></td></tr>
<tr><td>指定地域密着型介護予防サービス事業者</td><td></td><td></td></tr>
<tr><td>指定介護予防支援事業者</td><td></td><td></td></tr>
<tr><td>みなし指定</td><td>義務ではないが、みなし指定の認識をさせるため、自治体独自に通知書を発行している場合あり。</td><td>介護保険事業所番号（10 桁）

※3 桁+保険医療機関コード（7 桁）</td><td>保険医療機関・保険薬局の指定の有効期間（6 年）に順ずる。</td></tr>
</table>

1）介護保険事業所番号

介護事業所番号の構成は図表 2-13 の通りで、10 桁で構成される。

図表 2-13　介護保険事業所番号の構成[4]



このように、同一事業所に複数の介護保険事業所番号が存在する場合がある点に留意が必要である。また自治体へのヒアリング結果から、以下のことが分かった。

- 介護保険事業所番号は、事業所毎に発行される。
- 同一事業所とは、事業所名と事業所所在地が同じ場合。
- 同一事業所で複数の介護サービスを提供する場合も、事業所区分番号が異なるサービスであれば、基本は新たに採番される。ただし事業所が希望すれば、その事業所へ既に採番されている番号を使うこともできる。
- 介護保険事業所番号の再利用は無い。廃番として管理されている。

以上より、介護事業所番号は所在地毎に異なり、一度採番された番号は再利用されないことが分かった。

2）介護事業者の指定以外の主な手続

介護事業者の指定を受けた後の主な手続は図表 2-14 の通りである。事業所に関する変更において、指定権者をまたぐ事業所の移転（同一所在地で複数の介護保険サービス事業を同一事業所番号で運営しており、その一部の事業を移転）の場合、介護保

[4]出典：独立行政法人福祉医療機構資料「介護予防・日常生活支援総合事業における事業所番号の考え方について」。

険事業所番号が変更になる。

図表 2-14　介護事業所指定後の主な手続概要

各種手続種別	詳細	備考
「事業所」に関する変更手続	・事業所の名称の変更 ・事業所の所在地の変更 ・事業所の電話番号、FAX 番号の変更 ・事業所の平面図の変更（専用区画、レイアウト） ・管理者の氏名及び住所の変更 ・介護支援専門員の氏名及び登録番号の変更 ・運営規程の変更　等	指定権者をまたぐ事業所の移転 （同一所在地で複数の介護保険サービス事業を同一事業所番号で運営しており、その一部の事業を移転する場合、事業所番号が変更になる）。
「法人」に関する変更手続	・法人の名称の変更 ・法人の所在地の変更 ・法人の電話番号、FAX 番号の変更 ・代表者の変更 ・代表者の住所の変更 ・役員の変更 ・役員の住所の変更 ・定款・寄付行為・条例等の変更（当該指定事業に関するものに限る）等	統合等により別法人となる場合は、変更の扱いとはならない。 旧事業所を廃止し、新たな法人による新規申請が必要となる。
事業所の廃止・休止手続	・廃止したとき ・休止したとき	指定と廃止情報は公示義務あり。 公示方法は各自治体による。
休止事業所の再開手続	・再開しようとするとき	
指定辞退の手続	・指定を辞退しようとするとき	
事業所の指定更新手続	・再指定を申請するとき（6 年毎）	

2.4.3. 認定基準について

（１）認定基準の考え方

接続機関の認定基準として以下２つの項目の確認が必要であると考えられる。

1)　実在性の確認

接続機関が確実に存在していること。

2) 有資格性の確認
接続機関が全国保健医療情報ネットワークに接続する要件を満たしていること。後述「3.12.1 セキュリティ規程」で記述する。

（２）介護事業者、保険医療機関、保険薬局の認定基準

調査結果から、介護事業者は所管する都道府県・市町村から、保険医療機関、保険薬局は所管する地方厚生局から「指定通知書」が発行されていることが明らかになった。そのため、介護事業者、保険医療機関、保険薬局であることの認定基準は、①「指定通知書」を有しており、②「指定通知書」が有効であることとすることが考えられる。

指定通知書を確認することにより、当該介護事業者、保険医療機関、保険薬局が確実に存在していること及び介護事業者、保険医療機関、保険薬局であるという資格を有していることが同時に証明できる。

何らかの理由で「指定通知書」が確認できない場合は、紛失時は再発行を依頼することが考えられるが、再発行以外の場合、HPKI-CP で定めている基準を踏襲することが考えられる。HPKI-CP では、登記事項証明書、保険医療機関等の開設時に提出した開設届の副本のコピー、開設許可証等、公的機関から発行もしくは受領した証明書、各法等で提示を求められているもののコピーのいずれかにより実在性の確認を行うことが定められている。さらに資格の確認のため、介護事業者、保険医療機関、保険薬局であることを証明する書類として、診療報酬の支払後、審査支払機関から発行される直近 3 ヶ月以内の支払通知書のコピーを確認することが考えられる。しかし、介護事業者、保険医療機関、保険薬局であれば確実に「指定通知書」を保有しているため、「指定通知書」が確認できない場合については認定基準として採用しないこととした。ただし、実務上は保険医療機関でないケース（遠隔診療のみ実施している機関等）も考えられるため、今後の検討課題である。

（３）地連事業主体、サービス事業者の認定基準

参考文献(3)において、地連事業主体の組織要件が述べられており、本事業における接続機関も同様の要件が求められると考える。

地域間連携を行うために接続を求める地連事業主体は、地域間連携において発生するさまざまな事象に対して運営の責任主体としても、また発生した事象によっては法的な責任を負う必要がある。この責任の所在を法的にも明確にするためには、事業主体は、法人であるか、もしくは個人事業主であることが必要である。

このことから、地連事業主体及びサービス事業者に求める要件は、法人または個人事業主であることを確認することにより実在性を確認する。また、セキュリティ基準に準拠していることを確認することにより有資格性を確認する。セキュリティ基準に

ついては、後述「3.12.1 セキュリティ規程」で記述する。なお、コンソーシアム等の、複数の企業、個人またはその他の組織の集合からなる団体に関しては、責任の所在が不明確になるため、接続機関の対象から除外する。

2.5. 認証主体の運用方法

（１）運用方法

運用開始までに決めなければならないと想定される主な項目を以下に記述する。

- 認証主体を決定する。
- 登録局と発行局の役割を整備する。
- 認証主体における認証局運用に必要な体制及び設備（データセンタ等）を整備する。
- 証明書の発行・失効や配付、その他認証局に必要となる運用フローを整備する。
- 認証局運用規程を策定する。
- 事務取扱要領を作成する。
- HPKI 準拠性審査を受ける。
- 証明書の料金及び徴収方法を決定する。

運用開始後に必要になると想定する主な業務を記述する。

- 認証局運用規程及び事務取扱要領に従い「2.2 認証主体の業務」を実施する。
- 定期的（1 年以内）に内部監査を実施する。
- 2 年に 1 回 HPKI 準拠性監査を受ける。
- 証明書料金の出納管理を行う。
- 必要に応じてヘルプデスクの体制を整備する。

（２）認証主体の機能

認証主体は大きく登録局と発行局の 2 つの機能から構成される。

ヘルプデスクについては必須の機能ではなく、接続機関からの問い合わせ対応の業務負荷に応じて設置するものである。ヘルプデスクの業務内容は、接続機関の申請方法等の登録局に関する内容が主と想定されるため、登録局での問い合わせ対応業務負荷に応じて、ヘルプデスクの体制が整備されるものと想定する。

1) 登録局
接続機関からの申請受付や接続機関の実在性・有資格性等の審査を実施する機能

2)　発行局

機関認証用証明書の発行及び失効を実施する機能（データセンタを想定）

3)　ヘルプデスク

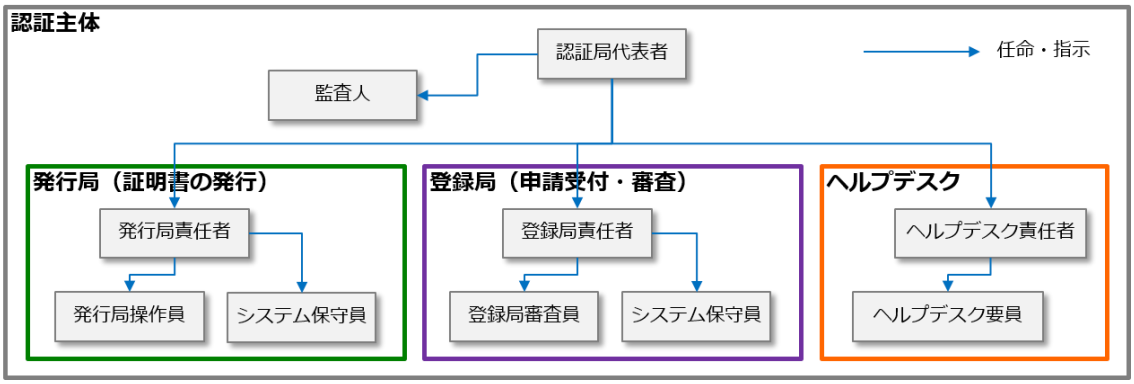
接続機関からの機関認証用証明書の発行や失効、使用方法等に関する問い合わせ窓口機能

なお、認証主体は、登録局、発行局及びヘルプデスクの運用を、認証主体の責任のもと外部組織に委託することを可能とする。

（３）認証主体の体制・役割

認証主体を運用するにあたり、最低限必要と考えられる体制と人員構成を図表 2-15 図表 2-15、図表 2-16 に示す。

図表 2-15　認証主体の体制図



図表 2-16　認証主体の人員構成例

所属	担当名	最低配置人数（案）	主な役割
認証主体	認証局代表者	1 名	運営主体の運営及び管理と業務の統括
	監査人	2 名	内部監査の実施
登録局	登録局責任者	1 名	登録局の運営及び管理と業務の統括
	登録局審査員	2 名	接続機関からの申請受付・審査
	システム保守員	1 名	登録局のシステム保守
発行局	発行局責任者	1 名	発行局の運営及び管理と

所属	担当名	最低配置人数（案）	主な役割
			業務の統括
	発行局操作員	2 名	機関認証用証明書の発行・失効
	システム保守員	1 名	発行局のシステム保守
ヘルプデスク（必要に応じて設置）	ヘルプデスク責任者	0 名	ヘルプデスクの運営及び管理と業務の統括
	ヘルプデスク要員	0 名	接続機関からの問合せ等の対応

2.6. 接続機関の廃業失効情報の管理方法

接続機関の廃業状況を知る方法としては以下の 3 つの方法が考えられる。認証主体の義務としてどこまでを実施するかは検討が必要であるが、通常の認証局の義務として（1）は必ず実施する必要がある。

（１）接続機関からの失効申請

接続機関の廃業後に不正利用されるリスクが無いよう、機関認証主体としては普段から廃業時の失効申請を周知する。

接続機関の義務として、本事業で作成する CP 及び認証主体が作成する CPS に「申請内容が虚偽なく正確であることに対する責任を果たすこと」を記載することにより、接続機関が失効申請を怠ったために発生した損害等については接続機関が責任を負うこととする。

（２）公的機関の公表情報を確認

1) 保険医療機関・保険薬局の場合
- 地方厚生局のホームページを確認する。

2) 介護事業者の場合
- 都道府県・市町村のホームページを確認する。（自治体により公開有無・公開タイミングが異なる。）
- 介護サービス情報公表システム[5]を確認する。（自治体により最新情報が反映されていない可能性がある。）

[5]介護サービス情報公表システムは、（http://www.kaigokensaku.mhlw.go.jp/）を指す。

3) 法人の場合
   - 国税庁の法人番号公表サイト[6]を確認する。

4) 個人事業者の場合
   - 公表情報がないため確認が出来ない。

いずれの場合も認証主体が確認するためには、統一されたデータベースがないと運用負荷が非常に高いと想定される。また、公開されるまでのタイムラグがあるためリアルタイムの確認が出来ない点に留意が必要である。

（３）第三者との情報連携

第三者機関（例えばネットワーク事業者）は利用料の滞納といった不利益を被る可能性があり、接続機関の廃業を知る必要性が高いため、ネットワーク事業者の接続機関へのサービス停止と連携し、その接続機関のサービス停止情報をネットワーク事業者から受ける方法が考えられる。

同様に、認証主体として証明書を月額利用料という形で徴収し、入金が滞った場合に失効対象とする方法も考えられる。

ただし、ネットワーク事業者のサービス停止が即接続機関の廃業にはならないケースもあるため、あくまで廃業の可能性が分かるに留まるため認証局側での確認はいずれにしても必要である。

2.7. 認証の主体の準拠性審査基準

本事業で実施した調査研究を踏まえ、HPKI-CP の見直しを実施し、見直し結果をもとに機関認証用（組織）の準拠性審査基準の素案を策定した。なお、準拠性審査基準素案のフォーマットは、「保健医療福祉分野ＰＫＩ認証局認証用証明書ポリシ準拠性審査業務実施規則 第 1 号様式に基づく監査報告書様式」（以下、参考文献(4)）をもとにしている。

なお、以下の観点から HPKI-CP の見直しを実施し準拠性審査基準素案を策定した。

1) 「保健医療福祉分野 PKI 認証局署名用証明書ポリシ 1.5 版」（以下、署名用 HPKI-CP）と「保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ 1.4 版」（以下、人認証用 HPKI-CP）との差異修正
2) 介護事業者、地連事業主体、サービス事業者の審査方法追加
3) 保険医療機関、保険薬局の審査方法整理
4) 介護事業者、地連事業主体、サービス事業者の hcRole 追加

[6]国税庁の法人番号公表サイトは、（http://www.houjin-bangou.nta.go.jp/）を指す。

5) 証明書プロファイルの最適化
6) 参照文献の最新化

策定した準拠性監査素案は、別冊「準拠性審査基準」参照。

3. 全国保健医療情報ネットワークに接続する機関認証方式

全国保健医療情報ネットワークに接続する機関について想定し、認証する方法について調査研究を実施した。

3.1. 機関認証用証明書記載情報（機関用 OID、hcRole(healthcare Role)）

HPKI-CP では、主な証明書プロファイルとして図表 3-1 が定められているが、以下の通り課題がある。

図表 3-1　HPKI-CP の証明書プロファイル

プロファイル項目（抜粋）		現版証明書ポリシ
SubjectDN		
	CountryName(C)	JP 固定
	LocalityName(L)	都道府県
	OrganizationName(O)	運営団体名
	OrganizationalUnitName(OU)	医療福祉機関の種類
	CommonName(CN)	医療機関名
	SerialNumber(SN)	医療機関番号等
SubjectDirectoryAttributes		hcRole 属性 ・ insurance medical care facility：保険医療機関 ・ insurance pharmacy：保険薬局

1) 医療機関番号等ユニーク ID を入れる項目として SerialNumber（以下、SN）が想定されており、同一医療機関で複数支店あるような場合は SN が同一になってしまう。SN を使用して接続機関を単一に識別することができない。
2) 本事業の調査研究事項である機関用 OID 情報をユニーク ID にすることが考えられるが、SN を使ってしまうと医療機関番号等を入れることができなくなるため項目追加が必要である。また OID を記述するデータ型「OBJECT IDENTIFIER」を格納する属性情報が X.501（参照規格(2)）や X.520（参照規格(3)）を調査したものの特定することができなかった。「Organizational Unit Name」「User ID」といった、データ型を「PrintableString」や「UTF8String」にできる属性情報の利用も考えられる。機関用 OID の属性に適った属性情報の割当てが必要である。
3) 証明書の検証側で、WEB サーバソフトや VPN 機器の仕様上、認証情報として特定の Subject 項目のみ利用可能な場合が考えられ、設計時に留意が必要である。
4) hcRole 属性として、「保険医療機関」「保険薬局」の 2 つのみ規定されており、本事業の調査研究事項でもある介護事業者、地連事業主体及びサービス事業者

を識別する必要がある場合は、hcRole の追加が必要である。どこまで分類するのか検討する必要がある。

3.1.1. 機関用 OID

多岐にわたる接続機関を認証するには一意に識別することが必要不可欠で一意の番号の在り方について過去に検討が行われてきた。参考文献(3)において、医療機関コードや法人番号を検討し、これらに依らない番号体系の必要性を述べており、一つの候補として国際的にも一意に識別可能な OID（object identifier、以下 OID）の活用が提案された。そこで、本事業において機関用 OID の活用方法と OID 証明書内の記載方法について検討した。

（１）OID 採番方法

厚生労働省では HPKI-CP に記載されている OID「1.2.392.100495」（＝MHLW）を所有しており、以下の通り採番されている。

- 1.2.392.100495.1 …JHPKI（保健医療福祉分野の公開鍵関連分野）
- 1.2.392.100495.1.5 …CA（保健医療福祉分野の認証局）
- 1.2.392.100495.1.5.1 …CP（保健医療福祉分野認証局の証明書ポリシ）

機関認証用に採番する階層を検討した結果、JHPKI の役割の 1 つと考えられることから、「1.2.392.100495.1」の下位に採番することとした。番号は CA が 5 であることから既に何種類かは採番されていることが考えられ、間隔をとり「100」とした。図表 3-2 に OID の採番案を示す。

図表 3-2　機関用 OID 採番方法（案）

OID	意味
1.2.392.100495.1.**100**	機関認証用 OID（=100）
1.2.392.100495.1.100.**1**	機関用 OID（=1）
1.2.392.100495.1.100.1.**1**	業種毎の OID で、保険医療機関・医科用（=1）
1.2.392.100495.1.100.1.**2**	業種毎の OID で、保険医療機関・歯科用（=2）
1.2.392.100495.1.100.1.**3**	業種毎の OID で、保険薬局用（=3）
1.2.392.100495.1.100.1.**4**	業種毎の OID で、介護事業者用（=4）
1.2.392.100495.1.100.1.**5**	業種毎の OID で、地連事業主体用（=5）
1.2.392.100495.1.100.1.**6**	業種毎の OID で、サービス事業者用（=6）
1.2.392.100495.1.100.1.x.**1**	同一業種内の機関毎の OID。医療機関番号（先頭に都道府県番号（2 桁）、点数表区分番号（1 桁）を連結した 10 桁固定の番号）や介護保険事業所番号、法人番号、または機関認証主体が採番するシ

OID	意味
	リアル番号
1.2.392.100495.1.100.1.x.x.1	同一業種内の機関毎の OID の枝番。法人番号等、機関の所在地毎に採番されない場合や医療機関番号等、番号が再利用される場合に利用。枝番を利用する条件は、 ・ 法人番号では、同一業種内の機関毎の OID が同じで所在地が異なる場合、機関認証主体が採番するシリアル番号 ・ 医療機関番号では、指定通知書に記載された「指定の期間」の開始日（8 桁固定の番号）

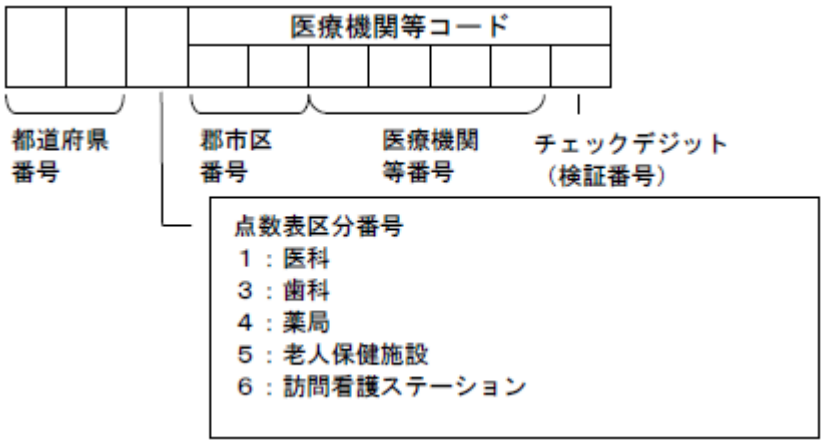
図表 3-2 の太枠で示した同一業種内の機関毎の OID の候補として、機関認証主体が採番するシリアル番号、または介護保険事業所番号や医療機関番号、法人番号といった採番済みの番号が考えられる。

検討した結果、採番管理の負担が少なく既に採番された番号の流用を考え、可能な場合は介護保険事業所番号や医療機関番号、法人番号を利用することとした。

また機関毎の OID を検討するなかで、医療機関番号について以下の 2 つの課題が分かり対策を検討した。

1) 7 桁の医療機関番号は図表 3-3 では「医療機関等コード」で、都道府県別でないため、都道府県が異なると重複する可能がある。
2) 医療機関番号が再利用される可能性がある。

図表 3-3 医療機関等コード（＝医療機関番号）を用いた事業所番号の構成[7]



課題 1)については、図表 3-3 やオンライン請求システム専用認証局の証明書におい

[7]出典：独立行政法人福祉医療機構資料「介護予防・日常生活支援総合事業における事業所番号の考え方について」。

て利用されている実績から、医療機関番号の先頭に都道府県番号（2 桁）、点数表区分番号（1 桁）を連結した 10 桁固定の番号にすることとした。同一業種内の機関毎の OID は図表 3-4 の通りになる。

図表 3-4　同一業種内の機関毎の OID（案）

業種		機関毎の OID
保険医療機関、保険薬局		都道府県番号（2 桁）、点数表区分番号（1 桁）及び医療機関番号（7 桁）を連結した 10 桁固定の番号[8]
介護事業者		介護保険事業所番号
地連事業主体、サービス事業者	法人	法人番号[9]
	個人事業主	機関認証主体で採番

課題 2)については、同一業種内の機関毎の OID の枝番を採番することで区別することが考えられ検討を行った。枝番とする番号として、異なる機関に対して同じ日に同じ医療機関番号が採番されることは無いと判断し、指定の開始日を用いる検討を行った。指定の開始日として、指定通知書に記載された「指定の期間」の開始日や、地方厚生局の公開情報である「コード内容別医療機関一覧表」に記載された、機関毎の「指定年月日」や「指定期開始」が考えられた。検討の結果、機関から申請された情報を証明書に記載することが適切と判断し、機関認証用証明書の申請書類の 1 つである指定通知書に記載された「指定の期間」の開始日を 8 桁固定で用いることとした。

（２）OID 格納場所

OID を記述するデータ型は「OBJECT IDENTIFIER」であるが、属性情報についての規格 X.501 や X.520 を調査した結果、OID を格納する適切な属性情報を特定することができなかった。このため、「Organizational Unit Name」「User ID」といった、データ型が「PrintableString」や「UTF8String」の属性情報の利用が考えられる。

また、証明書の検証側となる、WEB サーバソフトや VPN 機器の仕様を考慮する必要がある。標準機能で備わっている認証機能において、Subject 名のなかで認証情報として特定の属性情報のみ利用可能な場合がある。

例）

Apache…14 種類（Common Name、Organization Name、Organizational Unit Name、User ID、他）

CISCO ASA…19 種類（Common Name、Organization Name、Organizational

[8]医療機関番号利用時、機関毎の OID の下位で、指定通知書に記載された「指定の期間」の開始日を 8 桁固定の枝番を採番する。

[9] 法人番号利用時、同じ法人番号で所在地が異なる機関は、機関毎の OID の下位で、機関認証主体が枝番を採番する。

Unit、User ID、Serial Number、他）

以上より機関毎の OID としては、機関用属性情報として定義されていて、証明書の検証側で認証情報として利用可能な Organizational Unit Name が相応しいと考える。この場合、OID の一致確認は文字列比較となる。

3.1.2. hcRole

HPKI-CP の P.49「7.1.10 保健医療福祉分野の属性（hcRole)」に記載されている「保険医療機関」「保険薬局」以外の組織の分類について考察した。

hcRole 属性に設定する組織名として現在「保険医療機関」「保険薬局」の 2 種類が規定されている。本事業の調査研究事項である介護事業所や地連事業主体、サービス事業者を識別するためには組織名を追加する必要があり、図表 3-5 の通り定義した。

図表 3-5　hcRole 組織名（案）

組織名（hcRole）	説明
insurance medical care facility	保険医療機関
insurance pharmacy	保険薬局
insurance nursing care facility	介護事業者
regional medical information network service provider	地連事業主体
medical information service provider	サービス事業者

hcRole は証明書拡張情報 SubjectDirectoryAttributes に設定され、ASN.1 で記述される複雑なデータ構造となっている。現状では VPN 装置等で hcRole を処理することは難しいと思われるが、将来処理できるようになる可能性は考えられる。hcRole を規定した ISO 17090 準拠の証明書として、ネットワークレベル、アプリケーションレベル双方の機関認証用証明書に hcRole を記載するべきと考える。またサブジェクト名の中の属性情報に組織名を設定することで、WEB サーバソフトや VPN 機器に標準機能で備わっている認証機能においても組織名を識別可能になる。

3.1.3. プロファイル案

（１）証明書の有効期間

HPKI-CP では、「エンドエンティティの加入者の公開鍵証明書の有効期間は 2 年を越えないものとし、その私有鍵の使用は 2 年を越えないものとする。」と規定されている。一方で、人認証用 HPKI-CP 署名用 HPKI-CP では、最大 5 年と規定されている。

このため、人認証用 HPKI-CP と署名用 HPKI-CP に合わせる形で最大 5 年にすることが考えられるが、指定通知書の有効期間が 6 年であることを考慮すれば、保険医療機関・保険薬局・介護事業者に発行する機関認証用証明書は最大 6 年に設定することが考えられる。ただし、更新後の指定通知書が当該保険医療機関・保険薬局・介護事業者に通知され、通知後に更新後の指定通知書を用いて機関認証用証明書の継続（更新）申請をすることを考慮すると、指定通知書の有効期間と機関認証用証明書の有効期間を全く同じにした場合は、機関認証用証明書の有効期限が切れる前までに、継続（更新）申請が間に合わない、間に合った場合でも機関認証用証明書の発行が間に合わない等のケースが考えられる。そのため、更新後の指定通知書を用いた審査が可能な期間を考慮すると、機関認証用証明書の有効期間は 6 年+α にすべきと考えられる。

更新後の指定通知書が、更新前の指定通知書の有効期間満了後に通知される可能性があり遅くても有効期間満了後の 1 ヶ月後に通知され、その更新情報が各所管の公開情報に反映されるのが翌月と想定した場合、保険医療機関・保険薬局・介護事業者からの継続（更新）申請から機関認証主体での審査を考慮すると、機関認証用証明書の有効期間は、6 年と 3 ヶ月から 5 ヶ月程度にしておくべきと考えられる。

その場合、地連事業主体とサービス事業者向けの有効期間をどうするか検討する必要ある。以下の 3 つの案が考えられる。

1) 最大 6 年 5 ヶ月にあわせる。
2) 指定通知書のように有効期間がある書類で審査が出来ないため、人認証用 HPKI-CP と署名用 HPKI-CP に合わせて 5 年にする。
3) 有資格性の立証に使用すると想定される一般社団法人保健医療福祉情報安全管理適合性評価協会（以下、HISPRO）の「民間事業者による医療情報の外部保存及び ASP・SaaS サービス」適合性評価の有効期間である 2 年に合わせて 2 年にする。

認証主体の証明書管理業務の運用負荷を考慮すると、保険医療機関・保険薬局・介護事業者と地連事業主体・サービス事業者で証明書の有効期間を変えない方が良いと考えられる。また、保険医療機関・保険薬局・介護事業者との不公平さが生じる点も望ましくない。しかし、地連事業主体・サービス事業者については、「廃業届」の手続がないため認証主体が廃業を知る端緒がなく、証明書の有効期間内に廃業している可能性があると想定される。このため、証明書の有効期間は同一とするがその期間内により短いサイクルで実在性及び有資格性の確認は必要であると考える。

以上の検討の結果、証明書の有効期間は、以下の通りとすることが考えられる。

- 保険医療機関・保険薬局・介護事業者・地連事業主体・サービス事業者共に 6 年 5 ヶ月を越えないものとする。
- ただし、地連事業主体・サービス事業者については、少なくとも 2 年に 1 回程度、実在性及び有資格性の立証を認証主体に対して行うものとする。

この結果、本事業で作成する機関認証の証明書ポリシ（以下、新 HPKI-CP）では「エンドエンティティの加入者の公開鍵証明書の有効期間は 6 年 5 ヶ月を越えないものとし、その私有鍵の使用は 6 年 5 ヶ月を越えないものとする。」とすることが考えられる。

（２）サブジェクト名

医療機関番号等ユニーク ID を入れる項目として SN が想定されており、同一機関で複数支店あるような場合は SN が同一になってしまう可能性があり、SN を使用して接続機関を単一に識別することができない。そのため、本事業で検討している機関用 OID 情報をユニーク ID にすることが考えられるが、SN を使用すると医療機関番号等を入れることができなくなるため機関用 OID を格納するための項目追加が必要であり、格納する項目として図表 3-6 の通り「Organizational Unit Name（OU)」を追加することとした。

図表 3-6　サブジェクト名（案）

プロファイル項目（抜粋）		現版証明書ポリシ	新証明書ポリシ（案）
SubjectDN			
	CountryName(C)	JP 固定	JP 固定
	LocalityName(L)	都道府県	都道府県
	OrganizationName(O)	運営団体名	運営団体名
	OrganizationalUnitName(OU)	医療福祉機関の種類	医療福祉機関の種類
	OrganizationalUnitName(OU)	なし	認証局で採番する接続機関をユニークにする ID（機関用 OID）
	CommonName(CN)	医療機関名	接続機関名
	SerialNumber(SN)	医療機関番号等	医療機関番号／介護保険事業所番号／法人番号等

（３）SubjectAltName

SubjectAltName は HPKI-CP ではオプション項目である。

Subject 名の CN に「接続機関名」を入れる場合、WEB サーバ証明書やネットワーク用証明書（例えば VPN センタ装置側）等で必要となる FQDN 情報や IP アドレス情報を入れることができなくなるため、SubjectAltName の「DNSName」に FQDN 情報、「IPAddress」に IP 情報を入れることで対応することが考えられる。

なお、利用用途に応じた詳細な記載は、認証主体が作成する CPS で記載するものとし、新 HPKI-CP では図表 3-7 の通り HPKI-CP 同様にオプション項目とする。

図表 3-7　SubjectAltName（案）

プロファイル項目（抜粋）	現証明書ポリシ	新証明書ポリシ（案）	CPS（案）
SubjectAltName	△	△	△
DNSName	-	-	WEB サーバ用証明書、ネットワーク用証明書等の FQDN を格納
IPAddress	-	-	WEB サーバ用証明書、ネットワーク用証明書等の IP アドレスを格納

△：オプション項目、-記載しない

（４）KeyUsage／ExtendedKeyUsage

HPKI-CP では KeyUsage として「DigitalSignature」のみを設定することになっており、また「extendedKeyUsage」はオプション項目になっている。

本事業では WEB サーバやクライアント用の証明書の発行を想定することから「ExtendedKeyUsage」に「serverAuth」を設定することが考えられ、図表 3-8 図表 3-8 の記載の通り、KeyUsage として「KeyEncipherment」をオプション項目として追加する必要があると考える。なお、利用用途に応じた詳細な記載は、認証主体が作成する CPS で記載するものとし、新 HPKI-CP では HPKI-CP 同様にオプション項目とする。

図表 3-8　KeyUsage／ExtendedKeyUsage（案）

プロファイル項目（抜粋）	現証明書ポリシ	新証明書ポリシ（案）	CPS（案）
KeyUsage	◎	◎	◎
DigitalSignature	◎	◎	◎
KeyEncipherment	×	△	△ serverAuth の場合設定
ExtendedKeyUsage	△	△	△
serverAuth	-	-	WEB サーバの場合設定
clientAuth	-	-	WEB サーバ、クライアントの場合設定

◎：必須項目、△：オプション項目、×未使用項目、-記載しない

3.2. 発行対象別審査方法（法人、個人事業主、医療及び介護施設）

「2.4 接続機関の認定基準」を踏まえて検討した審査方法について、以下の 2 つの区分に発行対象を分けて述べる。審査内容は①実在性の確認、②申請意思の確認、③有資格性の確認の 3 項目の確認である。以下の 2 つに分けて審査方法を述べる。

- 保険医療機関・保険薬局・介護事業者の審査方法
- 地連事業主体、サービス事業者の審査方法

有資格性を確認することにより、当該資格に応じた hcRole を機関認証用証明書に格納する。

3.2.1. 保険医療機関、保険薬局、介護事業者の審査方法

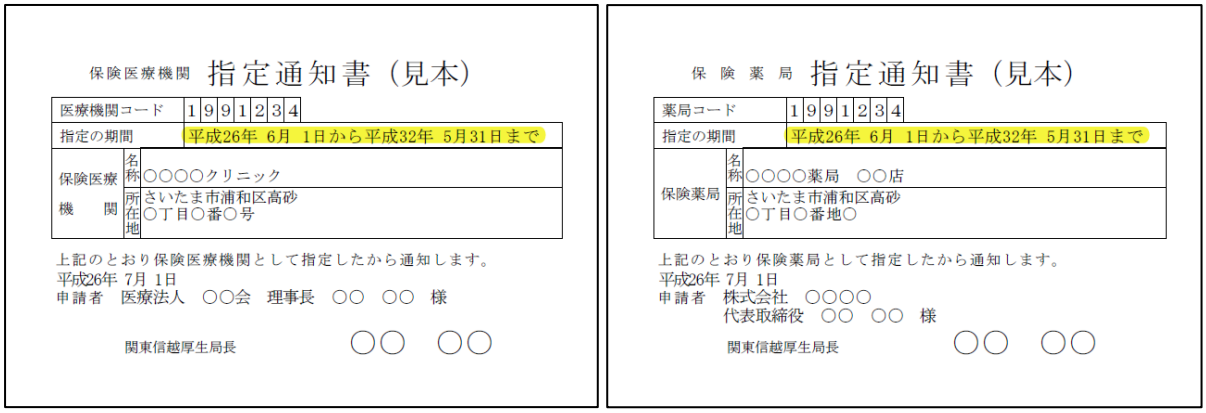
保険医療機関、保険薬局、介護事業者であることの確認に必要な書類及び方法を図表 3-9 に示す。また図表 3-10 に保険医療機関、保険薬局の指定通知書の見本、図表 3-11 に介護事業者の指定通知書の見本をそれぞれ示す。保険医療機関、保険薬局の指定通知書では、医療機関番号はそれぞれ、医療機関コード、薬局コードと記されている。

図表 3-9　保険医療機関、保険薬局、介護事業者の審査方法（案）

	保険医療機関	保険薬局	介護事業者
組織の実在性と有資格性	・指定通知書のコピー（有効期間内） 都道府県・市町村・地方厚生局等のホームページ[10]を確認し実在性と有資格性を確認		
組織の申請意思	・指定通知書のコピーに記載されている開設者の氏名と、当該組織の印（社印等）を認証局指定の申請書類に記名･押印 ・電子署名による確認 保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書、または、商業登記認証局の発行する電子証明書		
申請者の組織所属の確認	・組織の開設者と申請者が異なる場合 組織の申請意思を確認することにより組織所属の事実を立証		
申請組織の本部組織への所属確認	・所在地毎に指定通知書が発行されるので確認は不要		

[10]ホームページは、介護サービス情報公表システム（http://www.kaigokensaku.mhlw.go.jp/）を指す。

図表 3-10　保険医療機関、保険薬局の指定通知書（見本）[11]



保険医療機関　指定通知書（見本）

医療機関コード		1 9 9 1 2 3 4
指定の期間		平成26年 6月 1日から平成32年 5月31日まで
保険医療機関	名称	○○○○クリニック
	所在地	さいたま市浦和区高砂 ○丁目○番○号

上記のとおり保険医療機関として指定したから通知します。
平成26年 7月 1日
申請者　医療法人　○○会　理事長　○○　○○　様

関東信越厚生局長　　○○　○○

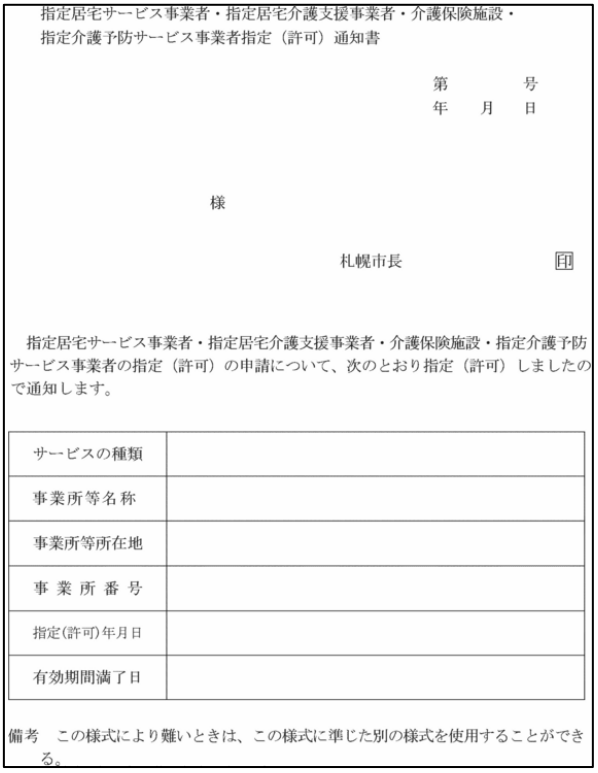
保険薬局　指定通知書（見本）

薬局コード		1 9 9 1 2 3 4
指定の期間		平成26年 6月 1日から平成32年 5月31日まで
保険薬局	名称	○○○○薬局　○○店
	所在地	さいたま市浦和区高砂 ○丁目○番地○

上記のとおり保険薬局として指定したから通知します。
平成26年 7月 1日
申請者　株式会社　○○○○
代表取締役　○○　○○　様

関東信越厚生局長　　○○　○○

図表 3-11　介護事業者の指定通知書（見本）[12]



指定居宅サービス事業者・指定居宅介護支援事業者・介護保険施設・
指定介護予防サービス事業者指定（許可）通知書

第　　号
年　月　日

様

札幌市長　　印

指定居宅サービス事業者・指定居宅介護支援事業者・介護保険施設・指定介護予防サービス事業者の指定（許可）の申請について、次のとおり指定（許可）しましたので通知します。

サービスの種類	
事業所等名称	
事業所等所在地	
事業所番号	
指定(許可)年月日	
有効期間満了日	

備考　この様式により難いときは、この様式に準じた別の様式を使用することができる。

[11]出典：関東信越厚生局ホームページ資料
https://kouseikyoku.mhlw.go.jp/kantoshinetsu/gyomu/bu_ka/shido_kansa/documents/shiteitsuuchisho.pdf。
[12]出典：札幌市ホームページ資料
http://www.city.sapporo.jp/ncms/reiki/d1w_reiki/412902100047000000MH/41290210004700000MH/S-20120611-047Z0002.rtf。

3.2.2. 地連事業主体、サービス事業者

（１）法人の場合

法人の種類は営利法人、非営利法人、公法人の大きく 3 種類あり、全ての種類の法人を対象とする。

図表 3-12　法人の種類

法人種類	営利法人	非営利法人	公法人
組織例	株式会社 特例有限会社 持分会社 合資会社 合同会社 等	一般社団法人 一般財団法人 医療法人 NPO 法人 事業共同組合 社会福祉法人 学校法人 等	国 地方公共団体 特殊法人 公団 公庫 道路公社 独立行政法人 国立大学法人 地方独立行政法人 公立大学法人 等
登記の要否	必要	必要	基本不要
法人番号	あり	あり	あり

法人であることを確認するために必要な書類及び方法を図表 3-13 に示す。

図表 3-13　法人の審査方法（案）

	営利法人	非営利法人	公法人
組織の実在性	・登記事項証明書 （発行日から 3 ヶ月以内）		登記がある場合 ・登記事項証明書（発行日から 3 ヶ月以内） 登記がない場合（添付書類不要） ・職員録あるいは官報での確認 ・国税庁法人番号公表サイト[13]での確認 上記で確認できない公法上の団体の場合 ・厚生局発行の公法人証明書
組織の申請意思	・当該組織の印（社印等）		・公印規則に定められた公印 公印規則で公印を確認することが出来ない場合

[13]国税庁法人番号公表サイトは、（http://www.houjin-bangou.nta.go.jp/）を指す。

	営利法人	非営利法人	公法人
			・職員録等で確認できる組織責任者名が記載されている別途認証局が定める書類に当該組織責任者の印
申請者の組織所属の確認	組織の代表者と申請者が異なる場合 ・組織の代表者の印が押印された申請書類にて組織所属の事実を立証		
申請組織の本部組織への所属確認	登記事項証明書が本部組織のみを証明している場合 ・組織代表者が地方組織名称を確認のうえ印を押すことにより所属していることの確認とする		組織の実在性確認で本部組織のみ証明している場合 ・組織代表者が地方組織名称を確認のうえ公印または当該組織責任者個人の印を押すことにより所属していることの確認とする

（２）個人事業主の場合

個人事業主であることの確認に必要な書類及び方法を図表 3-14 に示す。

図表 3-14　個人事業主の審査方法（案）

	個人事業主	備考
組織の実在性	以下いずれか１種類の書類	
	・青色または白色申告書のコピー	直近年のもの
	・個人事業の開廃業等届出書のコピー	直近のもの
	・所得税の青色申告承認申請書のコピー	直近年のもの
	・建設業の許可申請書または通知のコピー	直近のもの
	・測量業者登録申請書または通知のコピー	直近のもの
	・建築士事務所登録申請書または通知のコピー	直近のもの
	・（産業廃棄物及び一般廃棄物） 収集運搬業許可申請書または通知のコピー	直近のもの
	・（産業廃棄物及び一般廃棄物） 処分（処理）業許可申請書または通知のコピー	直近のもの
	・貨物自動車運送事業許可申請書または通知のコピー	直近のもの
	・貨物運送取扱事業許可申請書または通知のコピー	直近のもの
	・一般旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
	・特定旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
	・登録証明書等（測量業者登録証明書、建設コンサル	直近のもの

	個人事業主	備考
	タント現況報告書、地質調査業者現況報告書、補償コンサルタント現況報告書、建築士事務所登録証明書、土地家屋調査士登録証明書、計量証明事業者登録証明書、不動産鑑定業者登録証明書、弁理士登録証明書、司法書士登録証明書）のコピー	
	・納税証明書のコピー	直近年のもの
	・経営規模等評価結果通知書・総合評定値通知書のコピー	直近のもの
	・その他、公的機関またはこれに準ずる機関の印の付いた証明書、組織責任者の実印の付いた証明書、許可証等のコピー	直近のもの
組織の申請意思	・組織代表者個人の印	

3.3. 機関認証用証明書ライフサイクル別審査方法（新規発行、更新発行、再発行）

3.3.1. 機関認証用証明書の新規発行

新規発行とは、一度も機関認証用証明書を発行されたことがない接続機関に発行することである。また機関認証用証明書の証明書 Subject が変更となる場合で、再度証明書を発行する場合も新規発行とする。

「3.2 発行対象別審査方法（法人、個人事業主、医療及び介護施設）」に基づき、審査を実施する。

3.3.2. 機関認証用証明書の更新

更新（継続）とは、機関認証用証明書の有効期限が切れる前に、認証主体にて機関認証用証明書を新たに発行することであり、機関認証用証明書の Subject 情報を引きつぐことを想定している。

更新（継続）の方法として①認証主体による自動継続（クレジットカードのような運用）、②接続機関からの更新(継続)申請による更新（継続）の 2 つの場合が考えられる。

①の自動継続の場合は、接続機関側の手間は省けるが、既に当該接続機関が存在しない、または法人名・事業所名が変更になっている可能性があり、全国保健医療情報ネットワークの接続に使用する機関認証用証明書の更新方法としては、既に権限がない事業所に発行してしまう等のリスクが高いと考える。そのため、②の更新（継続）申請による方法が適していると考えられる。

更新（継続）時に必要となる申請書類は、更新（継続）時においても確実な実在性

を担保するために新規申請時と同じ書類を再度提出し、改めて認証主体で実在性等審査を実施することが望ましいと考える。

なお、同一接続機関であることの定義を以下に示す。

- 前回発行時と同じ保険医療機関名･保険薬局名・介護事業者名・法人名・個人事業主名
- 保険医療機関・保険薬局の場合は同じ医療機関番号
- 介護事業者の場合は同じ介護事業所番号

3.3.3. 機関認証用証明書の再発行

再発行とは、機関認証用証明書を格納した機器が壊れ機関認証用証明書が利用できなくなった場合等に、接続機関からの再発行申請に基づき機関認証用証明書を再発行することである。

再発行時の申請は、以下の 3 つの方法が考えられる。

1) 新規発行時と同じとする
2) 「発行通知書」による確認をする。
   発行通知書のコピーを認証主体に提出し、認証主体は当該発行通知書と紐付く証明書を発行する。
3) 機関認証用証明書情報公開サイトからの同一証明書をダウンロードさせる。
   発行通知書にダウンロード情報を記載しておき、接続機関は機関認証用証明書情報公開サイトにアクセスしいつでもダウンロード可能にしておく。

1)は確実な審査を実施できるが接続機関側の手間がかかる、認証主体側の審査手間もかかるうえ、機関認証用証明書の発行に時間がかかる。しかし、再発行時においても更新（継続）時と同様に確実な実在性を担保するためには、新規申請時と同じ書類を再度提出し、改めて認証主体で実在性等審査を実施することが望ましいと考える。

また、以下の点から再発行の必要性があるかどうかの検討も必要であり、本事業における再発行の扱いは、新規発行時と同様とした。

- 接続機関側で機関認証用証明書を管理可能であるため再発行は不要ではないか。
- 再発行が必要な場合は、接続機関側の法人格等変更で機関認証用証明書情報が変更になる場合＝新規発行の場合だけと考えることができないか。

3.3.4. 機関認証用証明書の失効

（１）機関認証用証明書の失効ケース

失効とは、機関認証用証明書の有効期間内に、何らかの理由により認証主体が機関認証用証明書を無効化することである。失効する方法として①接続機関からの失効申請による失効、②認証主体による強制失効の 2 つのケースが考えられる。

接続機関からの失効申請による失効とは、接続機関が廃業等により機関認証用証明

書を利用しなくなった場合、接続機関の情報が変更になった場合、機関認証用証明書を紛失した等が該当する。

認証主体による強制失効とは、認証主体が接続機関の廃業等を知った場合、認証主体が機関認証用証明書の不正利用を知った場合、認証主体が接続機関の認定基準を満たさなくなったことを知った場合、法令等で定められた組織から失効申請があった場合等が該当する。

（２）失効申請の審査方法

HPKI-CP 記載の通り失効申請時は以下を確認する。

- 失効を申請する証明書を特定する。
- 証明書を失効する理由を明らかにする。
- 失効申請書に認証局が検証可能な電子署名を付して認証局に送信する。
- 電子署名付きの申請ができない場合は、他の手段を用い加入者本人であることを立証する。

また、接続機関からの申請であることの確認は以下を確認する。

- 発行申請時と同じ責任者名と印を、失効申請書に記名・押印
- 介護事業所・保険医療機関・保険薬局の場合で責任者が変更になっている場合は、変更後の指定通知書のコピー
- 地連事業主体･サービス事業者で責任者が変更になっている場合は、責任者を証明する登記事項証明書等の提出

（３）失効の方法

失効の方法としては、以下 3 種類が考えられる。それぞれの方法について記載する。なお、下記 1)通常失効については、認証主体において必ず実施しなければならない。

1)　通常失効

HPKI-CP「4.9.1　証明書失効の要件」の＜組織管理者もしくは組織所属者、または代理人から失効申請があった場合＞において、接続機関からの失効申請に基づいて機関認証用証明書を失効する。

2)　緊急失効

接続機関内で不正アクセスが検出された場合や、地域医療情報連携ネットワーク内でウイルス感染が発覚した場合等、問題となる接続機関からのアクセスを直ちに停止する必要がある。その場合、接続機関、地域医療情報連携ネットワーク、またはネットワーク事業者のゲートウェイにて、問題となる接続元のアクセス制御設定を変更し対応することが望ましい。この場合の最終手段として、問題となる接続機関の機関認

証用証明書を失効させる方法が考えられ、認証主体としては緊急失効への対応は必要であると考える。

ただし、「通常失効」と異なり緊急性が求められるため、24 時間 365 日対応可能な窓口の設置や、緊急失効するための設備及び人員配備が必要となり、認証局運用コストが大幅にアップする可能性があるため、費用対効果を考慮した運用をしなくてはならない。

3) 一時失効

認証局での失効処理の方法として、一時失効という方法がある。例えば、上記 2)緊急失効の必要が生じた場合、当該機関認証用証明書を一時失効し、CRL に当該機関認証用証明書の情報を登録しておき、不正アクセスがなくなったので一時失効を解除して、CRL から当該機関認証用証明書情報を削除し、失効状態ではなくす方法が考えられる。

この場合、失効解除する判断が非常に困難になると想定される。問題となる接続機関からの失効解除申請だけでは、本当に失効解除していいかの判断が出来ず、何らかの方法（例えば第三者機関による確認）で技術的な判断を実施しなければならない可能性も生じる。

このような理由から、一時失効は実施しないほうがよいと考える。（HPKI-CP では一時失効は実施しないと規定されている）

3.4. 機関認証用証明書配付方法（オフライン時の対応）

3.4.1. 機関認証用証明書の種類

電子証明書は、電子証明書の生成方法により、①利用者側（接続機関）機器等でキーペアを生成、②機関認証主体（認証局）でキーペアを生成の 2 種類の形式での発行が可能である。機関認証主体が発行する電子証明書は、アプリケーション用証明書とネットワーク用証明書のどちらにも対応することを想定し、以下 2 種類いずれの形式にも対応する。

- 利用者側（接続機関）機器等でキーペアを生成　⇒　PKCS#7 形式
  機関認証主体は、接続機関からの PKCS#10 形式の申請情報データ（Certificate Signing Request、以下 CSR）に基づき、機関認証主体にて機関認証用証明書を生成する。生成した機関認証用証明書は、PKCS#7 形式ファイルで、接続機関責任者に別途定める安全な方法で受け渡しを行う。なお、本方法は接続機関にて公開鍵と私有鍵（活性化 PIN 含む）を生成するため、私有鍵の存在が接続機関であることが明らかであり、セキュリティ上安全な方法と考える。

- 機関認証主体（認証局）でキーペアを生成　⇒　PKCS#12 形式
  機関認証主体は、接続機関からの申請書類情報に基づき、機関認証主体にて機関認

証用証明書、公開鍵及びそれに対応した私有鍵（活性化 PIN 含む）を生成する。生成した機関認証用証明書、公開鍵及び私有鍵は、PKCS#12 形式ファイルで、接続機関に別途定める安全な方法で受け渡しを行う。なお、PKCS#12 形式ファイルは、私有鍵が含まれており、またコピー可能なファイルであるため、複数コピーされ不正利用される可能性があり、接続機関の厳格な管理が必要となる。

3.4.2. 機関認証用証明書の種類に対応したアプリケーション・機器と配布方法

アプリケーション用とネットワーク用の証明書に対応した配布方法を図表 3-15 に示す。

図表 3-15 機関認証用証明書種別の配布方法（案）

種別	想定利用用途 アプリケーション・機器	配付方法
アプリケーション用	WEB サーバ	・利用者側でキーペア生成 （PKCS#7）
	クライアント ・パソコン ・サーバ 等	・認証局側でキーペア生成 （PKCS#12）
ネットワーク用	・ルータ ・VPN ソフトウェア 等	

アプリケーション用の証明書の内、WEB サーバに設定して使用する WEB サーバ用証明書は、利用者側でキーペアを生成する。一般的にパブリック認証局が発行する WEB サーバ証明書は本方法で証明書を配布しているため、アプリケーションへの影響を考慮すれば本方法が適していると考える。ただし、本方法は接続機関側で証明書に格納する情報の一部（CSR）を生成するため、間違った情報が生成される可能がある。そのため認証局での CSR の確認が必要である。

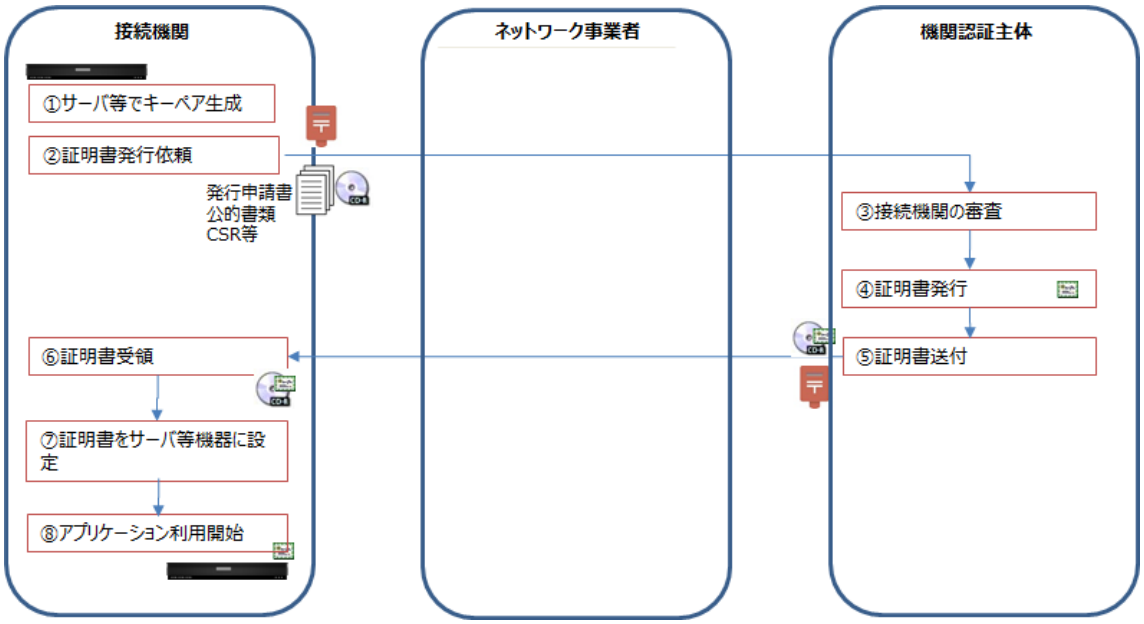
アプリケーション用の証明書の内、クライアントのアプリケーションとしてパソコンやサーバに設定して使用するクライアント用証明書や、ルータ等のネットワーク機器や VPN ソフトウェア等のネットワーク用ソフトウェアに設定して使用するネットワーク用証明書は、認証局側でキーペアを生成する。これらの利用用途は主にクライアント証明書として利用すると想定され、クライアント証明書情報を認証情報として使用するケースが考えられる。本方法は、認証局側で証明書に格納する全ての情報を生成するため、証明書情報の管理が利用者側でキーペア生成する場合と比べて容易で

あり、認証局側で確実に証明書をユニークにすることが可能である。そのため、クライアント証明書に利用する場合は、本方法が適していると考える。

ただし、接続機関側で厳重な私有鍵管理が必要であり、証明書の活性化 PIN は接続機関の知りえることが必要となる。

利用者側（接続機関）でキーペアを生成する場合の配布方法案を図表 3-16 に示す。なお WEB サーバ証明書を想定している。

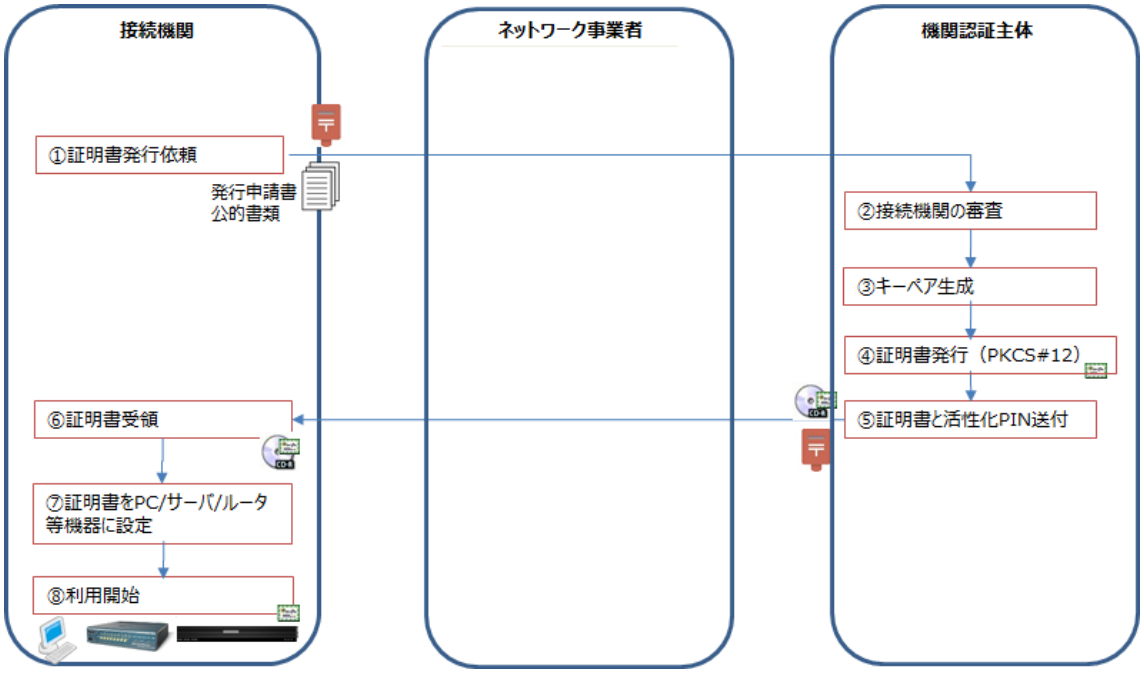
図表 3-16　機関認証用証明書（PKCS#7）の配布方法（案）



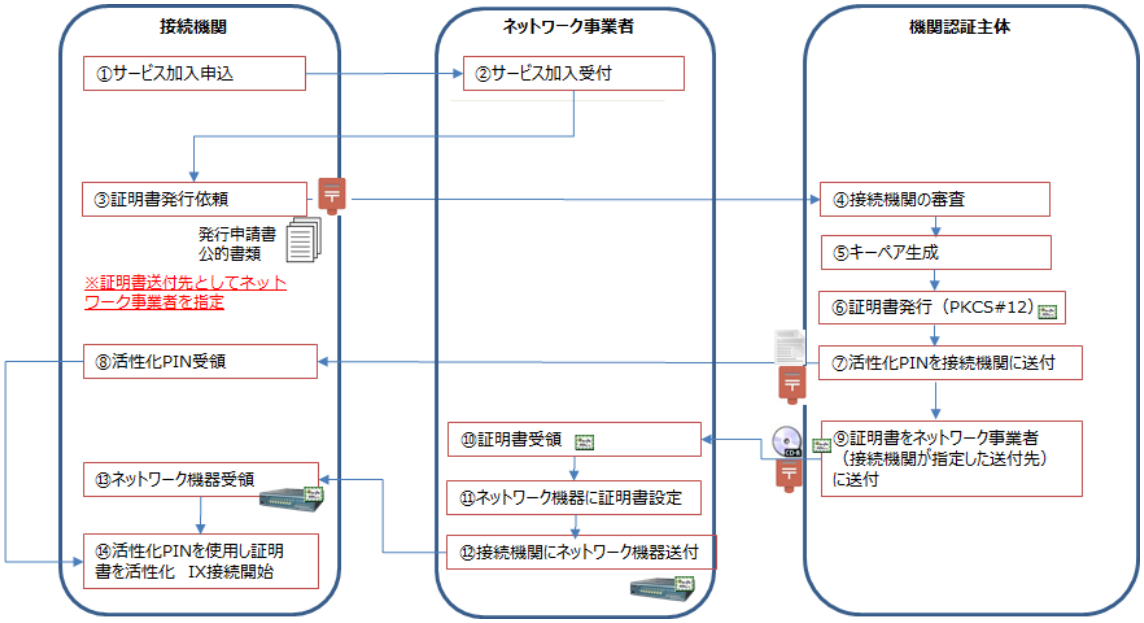
次に、機関認証主体（認証局）でキーペアを生成する場合の配布方法案を図表 3-17、図表 3-18、図表 3-19 の 3 通り示す。

1) 案①はクライアント用証明書及びネットワーク用証明書を想定している。
2) 案②はネットワーク用証明書を想定しており、全国保健医療情報ネットワークに接続するためにネットワーク事業者（本事業のネットワーク事業者の接続規定の要件を満たした事業者）との連携が必要な場合を想定している。なお、図表ではネットワーク機器としてルータを想定しているが、ネットワーク事業者が選定するルータ以外の機器や VPN ソフトウェアで利用するための USB トークンに格納する場合もあると想定している。
3) 案③は案②の応用でネットワーク事業者による代理申請の場合を想定している。

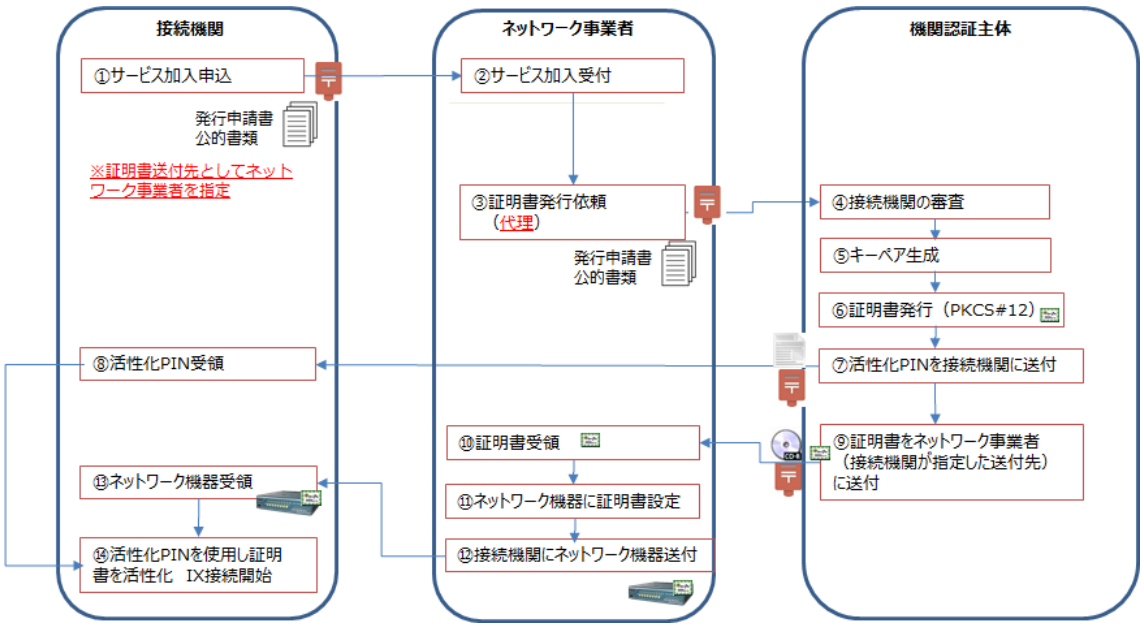
図表 3-17　機関認証用証明書（PKCS#12）の配布方法（案①）



図表 3-18　機関認証用証明書（PKCS#12）の配布方法（案②）



図表 3-19　機関認証用証明書（PKCS#12）の配布方法（案③）



3.5. 失効情報公開ポリシ

失効情報の公開ポリシは、HPKI-CP と同様に以下とした。

1) 認証主体が用意するリポジトリに失効リスト（Certificate Revocation List：CRL）として公開する。
2) CRL は、リポジトリにて http でアクセス可能とする。
3) CRL の有効期間は、有効期間 96 時間以内、48 時間以内更新とする。

3.6. ネットワークレベル証明書とアプリケーションレベル証明書との紐付け方法

（１）紐付け情報について

紐付け情報は本事業で検討した接続機関の証明書内に格納される機関用 OID が考えられる。紐付けが必要となる場面を想定し考察する。

（２）紐付ける場面について

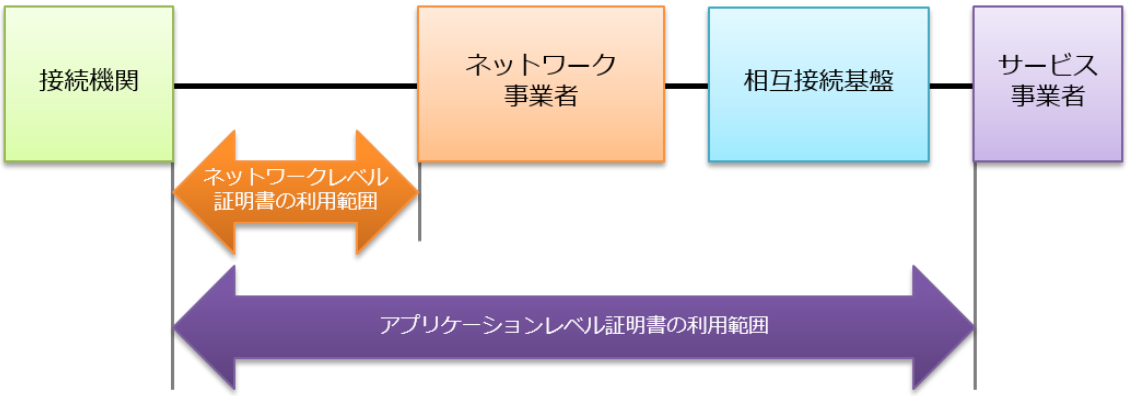
図表 3-20 の通り、ネットワークレベル証明書とアプリケーションレベル証明書の利用範囲は異なるため、通信中に紐付けることは難しい。

通信中であれば、ネットワーク事業者で、TLS 通信であればハンドシェイク中のクライアント証明書をキャプチャすることで紐付け可能と考えられる。ただし通信中の全メッセージのキャプチャ並びに解析の負荷が余計にかかることになる。

通信後であれば、通信ログを追跡するとき等が考えられる。ただし、ネットワーク

事業者、サービス事業者それぞれの通信ログに認証情報として機関用 OID が記録されることが前提となる。

図表 3-20　各機関認証用証明書の利用範囲



3.7. 現証明書ポリシとの差異の整理

以下の目的で、HPKI-CP の変更点を整理した。

1) 署名用 HPKI-CP と人認証用 HPKI-CP との差異修正
2) 介護事業者、地連事業主体、サービス事業者の審査方法追加
3) 保険医療機関、保険薬局の審査方法整理
4) 介護事業者、地連事業主体、サービス事業者の hcRole 追加
5) 証明書プロファイルの最適化
6) 参照文献の最新化

HPKI-CP と本事業により改定した新 HPKI-CP との差異を、図表 3-21 に示す。

なお、HPKI-CP には項目がなく、本事業により追記した項目については、「現版証明書ポリシ」欄は「項目なし」とし「本事業により改定（案）」欄に追記した文章を記載している。また、HPKI-CP に記載があり、本事業により文章中の文言の修正や追記している文章については、「本事業による改訂（案）」欄には下線を記載し表している。

図表 3-21　HPKI-CP の改定検討

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
全体	（項目なし）	・誤字脱字修正 ・表記のゆれを統一
1.1　概要 参照文章	署名用 HPKI-CP と人認証用 HPKI-CP と差異がある	・署名用 HPKI-CP と人認証用 HPKI-CP との差異修正 ・参照文献の最新化
1.5.2	【問い合わせ先】	【問い合わせ先】

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
問い合わせ	窓口：厚生労働省　医政局　政策医療課　医療技術情報推進室 受付時間：10 時～17 時（平日） 電話番号：03-3595-3412 FAX 番号：03-3501-5712 e-mail アドレス：hpki-cp@mhlw.go.jp	窓口：厚生労働省　政策統括官付情報政策担当参事官室 受付時間：10 時～17 時（平日） 電話番号：03-3595-2314 FAX 番号：03-3595-2198 e-mail アドレス：hpki-cp@mhlw.go.jp
3.1.5 名称の一意性	認証局が発行する電子証明書の加入者名（subjectDN）は、認証局内で一意にするためにシリアル番号（SN）を含むことができる。また、認証局の名称（issuerDN）は、保健医療福祉分野 PKI 内で、ある特定の認証局を一意に指し示すものである。	認証局が発行する電子証明書の加入者名（subjectDN）は、認証局内で一意にするためにシリアル番号（SN）もしくは OrganizationUnitName（OU）を含むことができる。また、認証局の名称（issuerDN）は、保健医療福祉分野 PKI 内で、ある特定の認証局を一意に指し示すものである。
3.2.2 組織の認証	保健医療福祉分野 PKI 認証局に保険医療機関等の組織の証明書を申請する際は、証明書の発行に先立ち、次のいずれかの方法で組織の実在性及び保険医療機関等であることを登録局に立証しなくてはならない。 なお、申請者個人の認証は「3.2.3 個人の認証」に定める方法による。	保健医療福祉分野 PKI 認証局に保険医療機関等の組織の証明書を申請する際は、証明書の発行に先立ち、次のいずれかの方法で組織の実在性及び保険医療機関等であることの有資格性を登録局に立証しなくてはならない。 なお、保険医療機関等ではない地域医療情報連携ネットワークの事業主体や医療情報共有サービスを提供する民間事業者等の場合は、組織の実在性と認証局が別途定義する有資格性を登録局に立証しなくてはならない。また、登録局は、地域医療情報ネットワークの事業主体、医療情報共有サービスを提供する民間事業者等に対しては、加入者証明書の発行から少なくとも 2 年に 1 度は、実在性及び

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		有資格性の確認書類の再提出を求めるものとする。
3.2.2 組織の認証	（項目なし）	＜保険医療機関、保険薬局、介護事業者の場合＞ 保険医療機関等の指定を受けた際に地方厚生局、都道府県、市町村から発行された指定通知書（有効期間内）のコピーを提出することによって組織の実在性を立証する。なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの有資格性の立証が同時になされたものとする。また、指定通知書のコピーには、申請時点において組織の開設者である者の氏名が記載されていなくてはならない。 ・電子証明書を用いる場合 前述の組織の運営区分に係わらず、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書を用いた電子署名により、実在性を立証することができる。 この場合、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書による電子署名を用いる場合は、同時に保険医療機関等であることの立証がなされたとみなすが、商業登記認証局の発行する電子証明書を用いる場合は、別途、指定通知書のコピーの提出を認証局が定める方法により提出しなくてはならない。

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		・法令等の要請により発行する場合 保健医療福祉分野 PKI 認証局が法令等の要請により、保険医療機関等の組織の証明書を発行する際は、法令で定められた機関が保険医療機関等の確認を実施し、その結果を登録局に提示することで組織の認証を実施しなくてはならない。
3.2.2 組織の認証	・法人組織の場合 商業登記簿謄本、保険医療機関等の開設時に提出した開設届の副本のコピー、保険医療機関等の指定を受けた際に地方厚生局より発行された指定通知書のコピー等公的機関から発行もしくは受領した証明書、各法等で提示を求められているもの※のコピーのいずれかを提出することによって組織の実在性を立証する。なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの立証が同時になされたものとするが、それ以外の証明書等で実在性を立証した場合、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピー等保険医療機関等であることを証明する書類の提出を必須とする。また、これらの立証の際に用いる各種書類には、申請時点において組織の管理者である者の氏名が記載され	＜保険医療機関、保険薬局、介護事業者以外の組織の場合＞ ・法人組織の場合 登記事項証明書を提出することによって組織の実在性を立証する。なお、所属する組織によって商業登記を本部組織でのみ行い、登記事象証明書が本部組織のみを証明している場合においては、本部組織の代表者が地方組織の名称を確認の上、認証局が指定する申込書に押印し認証局に提示することにより地方組織の実在性を立証する。また、別途認証局が指定する方法により有資格性の立証をする。

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	ていなくてはならない。	
3.2.2 組織の認証	・個人事業者の場合 商業登記簿謄本、保険医療機関等の開設時に提出した開設届の副本のコピー、保険医療機関等の指定を受けた際に地方厚生局より発行された指定通知書のコピー等公的機関から発行若しくは受領した証明書、各法等で掲示を求められているもの※のコピー若しくはそれらに順ずる書類のいずれかを提出することによって組織の実在性を立証する。 なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの立証が同時になされたものとするが、それ以外の証明書等で実在性を立証した場合、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピー等保険医療機関等であることを証明する書類の提出を必須とする。 また、これらの立証の際に用いる各種書類には、申請時点において組織の管理者である者の氏名が記載されていなくてはならない。 ＊「各法等で掲示を求められているもの」とは、以下のようなものを指す。 ・医療法　第 14 条の 2（院内掲示義務） ・薬事法施行規則　第 3 条（許	・個人事業者の場合 青色申告書のコピー、白色申告書のコピーや個人事業の開廃業等届出書のコピー等の組織情報を証明する書類を提出することによって組織の実在性を立証する。また、別途認証局が指定する方法により有資格性の立証をする。

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	可証の掲示） ・指定居宅サービス等の事業の人員、設備及び運営に関する基準　第 32 条及びその準用条項（掲示）	
3.2.2 組織の認証	・電子証明書を用いる場合 前述の組織の運営区分に係わらず、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書を用いた電子署名により、実在性を立証することができる。この場合、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書による電子署名を用いる場合は、同時に保険医療機関等であることの立証がなされたとみなすが、商業登記認証局の発行する電子証明書を用いる場合は、別途、指定通知書のコピー、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピー等保険医療機関等であることを証明する書類の提出を認証局が定める方法により提出しなくてはならない。	・電子証明書を用いる場合 商業登記認証局の発行する電子証明書を用いた電子署名により、法人組織の実在性を立証することができる。
3.2.2 組織の認証	・法令等の要請により発行する場合 保健医療福祉分野 PKI 認証局が法令等の要請により、保険医療機関等の組織の証明書を発行する際は、法令で定められた機関が保険医療機関等の確認を実施し、その結果を登録局に提示す	・法令等の要請により発行する場合 保健医療福祉分野 PKI 認証局が法令等の要請により、保険医療機関等<u>以外</u>の組織の証明書を発行する際は、法令で定められた機関が保険医療機関等の確認を実施し、その結果を登録局に提示することで

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	ることで組織の認証を実施しなくてはならない。	組織の認証を実施しなくてはならない。
3.2.3　個人の認証	保健医療福祉分野 PKI 認証局に証明書を申請しようとする際は、証明書の発行に先立ち、次のいずれかの方法で、組織管理者の実在性並びに申請者の実在性、組織所属の事実、組織の証明書申請意思を登録局に立証しなくてはならない。また、組織から委任を受けた者（以下、代理人）が申請する場合は、組織所属の事実に代えて組織からの申請委任の事実を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。 なお、本節の定めは証明書申請者の立証に関わる定めであり、登録局が証明書を発行する場合は、本節の規定に従い申請者の立証を行わせ、4 章の規定に則り申請者の審査及び証明書の発行を実施する。	保健医療福祉分野 PKI 認証局に証明書を申請しようとする際は、証明書の発行に先立ち、次のいずれかの方法で、組織の開設者もしくは代表者（以下、開設者と代表者を区別しない場合は総称して「管理者」と呼ぶ。）の実在性並びに申請者の実在性、組織所属の事実、組織の証明書申請意思を登録局に立証しなくてはならない。また、組織から委任を受けた者（以下、代理人）が申請する場合は、組織所属の事実に代えて組織からの申請委任の事実を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。 なお、本節の定めは証明書申請者の立証に関わる定めであり、登録局が証明書を発行する場合は、本節の規定に従い申請者の立証を行わせ、4 章の規定に則り申請者の審査及び証明書の発行を実施する。
3.2.3　個人の認証 ・組織管理者若しくは組織所属者が申請する場合	＜オンラインの場合＞ ２．申請者の実在性、組織所属の事実、組織の証明書申請の意思証明書を申請しようとする者は、認証局の定める手続に従い、保健医療福祉分野 PKI 認証局の発行する管理者向け署名用証明書を用いた電子署名により、申請者の実在性、組織所属の事実及び組織の証明書申請の	＜オンラインの場合＞ ２．申請者の実在性、組織所属の事実、組織の証明書申請の意思 証明書を申請しようとする者は、認証局の定める手続に従い、保健医療福祉分野 PKI 認証局の発行する管理者向け署名用証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書を用いた電子署名により、申請者の実在

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	意思を立証しなくてはならない。 　なお、保健医療福祉分野 PKI 認証局の管理者向け署名用証明書は組織の管理責任者に発行され、当該証明書による電子署名は、本人にしか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなす。	性、組織所属の事実及び組織の証明書申請の意思を立証しなくてはならない。 なお、当該証明書による電子署名は、本人にしか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなす。
3.2.3　個人の認証 3.代理人の申請	【1 点で確認できる書類】 ・日本国旅券 ・運転免許証 ・住民基本台帳カード（写真付のもの） ・戦傷病者手帳 ・海技免状 ・船員手帳 ・電気工事士免状 ・宅地建物取引主任者証 ・無線従事者免許証 ・猟銃/空気銃所持許可証 ・官公庁職員身分証明書 （張り替え防止措置済みの写真付）	【1 点で確認できる書類】 ・日本国旅券 ・運転免許証 ・住民基本台帳カード（写真付のもの） ・マイナンバーカード（個人番号カード） ・戦傷病者手帳 ・海技免状 ・船員手帳 ・電気工事士免状 ・宅地建物取引主任者証 ・無線従事者免許証 ・猟銃/空気銃所持許可証 ・官公庁職員身分証明書 （張り替え防止措置済みの写真付）
3.3.1 通常の鍵更新時の本人確認及び認証	加入者情報の通常の鍵更新は、「4.2.1　本人性及び資格確認」が実施された日から 5 年以内であれば、「3.2.3　個人の認証」で提出した書類または認証局で作成された記録を再び参照するか、加入者の署名を提示することで行える。 5 年を過ぎていた場合、もしくは元の書類もしくは記録が無効に	加入者情報の通常の鍵更新は、初回の証明書発行と同様の手順により申請するものとする。

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	なっているか廃棄されていた場合は、初回の証明書発行と同様の手順により申請するものとする。	
4.1.1　証明書の申請者	・保険医療機関等の組織からの申請により発行する場合 　証明書の申請者は、保険医療機関等の組織管理者若しくは当該組織所属者若しくは保険医療機関等の組織管理者から委任を受けた代理人とする。	・保険医療機関、保険薬局、介護事業者からの申請により発行する場合 　証明書の申請者は、保険医療機関等の組織開設者もしくは当該組織所属者もしくは保険医療機関等の組織管理者から委任を受けた代理人とする。
4.1.1　証明書の申請者	（項目なし）	・保険医療機関、保険薬局、介護事象者以外の組織からの申請により発行する場合 　証明書の申請者は、当該組織の代表者もしくは当該組織所属者もしくは組織代表者から委任を受けた代理人とする。
4.1.2 申請手続及び責任	・保険医療機関等の組織からの申請により発行する場合 証明書の利用を希望する組織は、認証局で定める以下のいずれかの手続によって証明書の利用申請を行う。	・保険医療機関、保険薬局、介護事象者からの申請により発行する場合 証明書の利用を希望する組織は、認証局で定める以下のいずれかの手続によって証明書の利用申請を行う。
4.1.2 申請手続及び責任	1.持参 　保険医療機関等の組織管理者若しくは当該組織所属者若しくは代理人が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定める書類を持参することにより利用申請を行う。	1.持参 　保険医療機関等の組織開設者もしくは当該組織所属者もしくは代理人が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定める書類を持参することにより利用申請を行う。 なお、代理人による申請の場合

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	なお、代理人による申請の場合は、証明書の利用申請に必要な書類に加え、保険医療機関等の組織管理者による委任状及び本CP「3.2.3 個人の認証」の代理人が申請する場合に定める代理人の本人性を確認可能な書類も同時に提出するものとする。	は、証明書の利用申請に必要な書類に加え、保険医療機関等の組織開設者による委任状及び本CP「3.2.3 個人の認証」の代理人が申請する場合に定める代理人の本人性を確認可能な書類も同時に提出するものとする。
4.1.2 申請手続及び責任	2.郵送 保険医療機関等の組織管理者若しくは当該組織所属者が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局が定める書類を郵送することにより利用申請を行う。 なお、代理人による郵送での申請は認めない。	2.郵送 保険医療機関等の組織開設者もしくは当該組織所属者が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局が定める書類を郵送することにより利用申請を行う。 なお、代理人による郵送での申請は認めない。
4.1.2 申請手続及び責任	3.オンライン 保険医療機関等の組織管理者が登録局にオンラインで「3.2.2 組織の認証」、「3.2.3　個人の認証」及び認証局の定めるデータを送付することにより利用申請を行う。 なお、当該組織所属者及び代理人によるオンラインでの申請は認めない。	3.オンライン 保険医療機関等の組織開設者が登録局にオンラインで「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定めるデータを送付することにより利用申請を行う。 なお、当該組織所属者及び代理人によるオンラインでの申請は認めない。
4.1.2 申請手続及び責任	（項目なし）	・保険医療機関、保険薬局、介護事象者以外の組織からの申請により発行する場合 証明書の利用を希望する組織は、認証局で定める以下のいずれかの手続によって証明書の利用申請を行う。 1.持参 組織の代表者もしくは当該組織

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		所属者もしくは代理人が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定める書類を持参することにより利用申請を行う。 　なお、代理人による申請の場合は、証明書の利用申請に必要な書類に加え、組織代表者による委任状及び本 CP「3.2.3 個人の認証」の代理人が申請する場合に定める代理人の本人性を確認可能な書類も同時に提出するものとする。 2.郵送 組織の代表者もしくは当該組織所属者が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局が定める書類を郵送することにより利用申請を行う。 なお、代理人による郵送での申請は認めない。 3.オンライン 　組織の代表者が登録局にオンラインで「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定めるデータを送付することにより利用申請を行う。 　なお、当該組織所属者及び代理人によるオンラインでの申請は認めない。 また、証明書の利用申請者は、申請にあたり、本 CP「1.3 PKI の適用範囲」と第 9 章で規定される認証局の責任範囲を理解し、同意した上で利用申請を行うものとする。更に、本 CP に則り運営される、各認証局の定める開示文書及び利用約款等も利用申請の前に読

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		み、内容を理解し、それらに同意した上で利用申請を行うものとする。
4.2.1　本人性及び資格確認	1.組織への証明書発行 認証局は、組織への証明書の発行時、本 CP「3.2.2　組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。	<保険医療機関、保険薬局、介護事業者からの申請により発行する場合> 　認証局は、組織への証明書の発行時、本 CP「3.2.2　組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。
4.2.1　本人性及び資格確認	・組織管理者もしくは組織所属者からの申請の場合 （1）持参の場合 申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れてないことの確認を実施する。また、申請者が組織管理者でない組織所属者の場合、社員証等の組織所属の証明書を所持していれば提示を求め、所持していない場合は、申請書に記載されている組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、保険医療機関等であることの確認は、地方厚生局が所管し公開してい	・組織開設者もしくは組織所属者からの申請の場合 （1）持参の場合 申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れてないことの確認を実施する。また、申請者が組織開設者でない組織所属者の場合、社員証等の組織所属の証明書を所持していれば提示を求め、所持していない場合は、申請書に記載されている組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、保険医療機関等であることの確認は、地方厚生局が所管し公開している、全保

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	る、全保険医療機関・保険薬局一覧等を用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認してもよい。 なお、確認に用いた証明書等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。	険医療機関・保険薬局一覧等を用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認してもよい。 なお、確認に用いた証明書等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。
4.2.1　本人性及び資格確認	（2）郵送の場合 申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れていないことの確認を実施する。また、申請書記載の組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、保険医療機関等であることの確認は、地方厚生局が所管し公開している、全保険医療機関・保険薬局一覧等を用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信	（2）郵送の場合 申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れていないことの確認を実施する。また、申請書記載の組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、保険医療機関等であることの確認は、地方厚生局が所管し公開している、全保険医療機関・保険薬局一覧等を用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすること

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認してもよい。 なお、証明書の受け渡しに関して、申請者本人が登録局に出頭する場合は、電子証明書若しくは電子証明書を生成する符号を窓口で交付することにより実在性の確認を実施する。郵送で交付する場合は、電子証明書若しくは電子証明書を生成する符号を申請者本人へ本人限定受取郵便で送付することにより実在性の確認を行う。 なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。	が可能な場合は、それを用いて確認してもよい。 なお、証明書の受け渡しに関して、申請者本人が登録局に出頭する場合は、電子証明書もしくは電子証明書を生成する符号を窓口で交付することにより実在性の確認を実施する。郵送で交付する場合は、電子証明書もしくは電子証明書を生成する符号を申請者本人へ本人限定受取郵便（特例型）等郵送記録が確実に残る方法で送付することにより実在性の確認を行う。 なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。
4.2.1　本人性及び資格確認	（項目なし）	<保険医療機関、保険薬局、介護事業者以外の組織からの申請により発行する場合> 　認証局は、組織への証明書の発行時、本 CP「3.2.2　組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。 ・組織代表者もしくは組織所属者からの申請の場合 (1)持参の場合 　申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れてないことの確認を実施する。また、申請者が組織代表者でない組織所属者の場合、社員証等の組織

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		所属の証明書を所持していれば提示を求め、所持していない場合は、申請書に記載されている組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、法人組織であることの確認は、国税庁が所管し公開している、法人番号公表サイトを用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認してもよい。 なお、確認に用いた証明書等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。 (2)郵送の場合 申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れていないことの確認を実施する。また、申請書記載の組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。 ただし、組織が中央官庁・地方公

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略することができる。 また、確認内容の内、法人組織であることの確認は、国税庁が所管し公開している、法人番号公表サイトを用いて確認することも可能である。 もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認してもよい。 なお、証明書の受け渡しに関して、申請者本人が登録局に出頭する場合は、電子証明書もしくは電子証明書を生成する符号を窓口で交付することにより実在性の確認を実施する。郵送で交付する場合は、電子証明書もしくは電子証明書を生成する符号を申請者本人へ本人限定受取郵便で送付することにより実在性の確認を行う。 なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。 (3)オンラインの場合 登録局から当該申請者の電子署名の有効性の確認を実施する。 この場合においても、法人組織であることの確認は、国税庁が所管し公開している、法人番号公表サ

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		イトを用いて確認することも可能である。もしくは、同等の信頼のおける台帳やデータベースを保有している機関に問合せをして確認してもよい。 なお、確認に用いた電子署名の付与された申請書は、登録局で保存年限を定めて保存しておくものとする。 ・代理人からの申請の場合 (1)持参の場合 代理人から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れてないことの確認を実施する。また、申請書に記載されている組織の電話番号に電話し、組織及び申請者が存在することを確認し、更に代理人に対する委任の事実を確認する。 ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類及び委任状を確認することで、問い合わせによる確認を省略することができる。 加えて、代理人に「3.2.3　個人の認証　・代理人が申請する場合」の＜持参の場合＞に定める本人性を確認する書類の提示を求め、対面による代理人の本人性の確認を実施する。 この場合も、1 点の書類で確認できる場合と 2 点の書類で確認が必要な場合があり、必要な書類につ

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
		いては各認証局が選択し、CPS で定めることとする。 　また、確認内容の内、法人組織であることの確認は、国税庁が所管し公開している、法人番号公表サイトを用いて確認することも可能である。 　なお、確認に用いた証明書等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。 (2)郵送の場合 　認証局は、代理人による郵送の申請を認めない。 (3)オンラインの場合 認証局は、代理人によるオンラインの申請を認めない。
4.2.1　本人性及び資格確認	・法令等の要請により証明書を発行する場合 本人性（組織）及び資格の確認については、法令等で定められた組織が保険医療機関等の実在性、保険医療機関等であることの認証を実施した結果を持って資格確認に変えることができる。	<法令等の要請により証明書を発行する場合> 本人性（組織）及び資格の確認については、法令等で定められた組織が当該組織の実在性及び有資格性があることの認証を実施した結果を持って資格確認に変えることができる。
4.3.1　証明書発行時の認証局の機能	＜認証局が鍵ペアを生成する場合＞ 認証局が鍵ペアを生成する場合は、「電子署名及び認証業務に関する法律施行規則」第 6 条第三号に準じて CPS 及び事務取扱要領を規定し、運用する。 CPS 及び事務取扱要領の規定としては、最低限以下の項目を含	＜認証局が鍵ペアを生成する場合＞ 認証局が鍵ペアを生成する場合は、「電子署名及び認証業務に関する法律施行規則」第 6 条第三号に準じて CPS 及び事務取扱要領を規定し、運用する。 CPS 及び事務取扱要領の規定としては、最低限以下の項目を含める

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	めるものとする。 １．加入者鍵ペアの生成は、認証設備室と同等の安全性が確保できる環境下で行い、アクセス権限管理、内部けん制等によりセキュリティ対策を講じていること。 ２．加入者鍵ペアの転送や出力を行う場合も、十分なセキュリティ対策を講じていること。 また、加入者鍵ペアを転送、出力した後は、速やかに加入者鍵ペアを完全に廃棄若しくは消去すること。 ３．加入者鍵ペアの活性化に使用する PIN 等の生成、転送、出力等を行う場合も、十分なセキュリティ対策を講じていること。 また、PIN 等を生成、転送、出力した後は、速やかに PIN 等を完全に廃棄若しくは消去すること。	ものとする。 １．加入者鍵ペアの生成は、認証設備室と同等の安全性が確保できる環境下で行い、アクセス権限管理、内部けん制等によりセキュリティ対策を講じていること。 ２．加入者鍵ペアの転送や出力を行う場合も、十分なセキュリティ対策を講じていること。 また、加入者鍵ペアを転送、出力した後は、速やかに加入者鍵ペアを完全に廃棄もしくは消去すること。 ３．加入者鍵ペアの活性化に使用する PIN 等の生成、転送、出力等を行う場合も、十分なセキュリティ対策を講じていること。 また、PIN 等を生成、転送、出力した後は、速やかに PIN 等を完全に廃棄もしくは消去すること。 ４．加入者鍵ペアの活性化に使用する PIN を加入者に通知する必要がある場合は、加入者にのみ確実に通知する対策を講じていること。
6.1.5 鍵のサイズ	エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズムまたは技術的に同等のアルゴリズムの場合、1024 ビットとする。他のアルゴリズムを使用するエンドエンティティの証明書の鍵の最小サイズは、同等	エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズムまたは技術的に同等のアルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用するエンドエンティティの証明書の鍵の最小サイズは、同等のセキュリティ

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	のセキュリティを提供するサイズとする。	を提供するサイズとする。
6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間	CA 公開鍵証明書の有効期間は 20 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。 エンドエンティティの加入者の公開鍵証明書の有効期間は 2 年を越えないものとし、その私有鍵の使用は 2 年越えないものとする。	CA 公開鍵証明書の有効期間は 20 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。 エンドエンティティの加入者の公開鍵証明書の有効期間は 6 年 5 ヶ月を越えないものとし、その私有鍵の使用は 6 年 5 ヶ月を越えないものとする。
7.1.3 アルゴリズムオブジェクト識別子	基本領域の Signature アルゴリズムは以下の通りとする。 sha1WithRSAEncryption (1.2.840.113549.1.1.5) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) 基本領域の subjectPublicKeyInfo アルゴリズムは以下の通りとする。 RSAEncryption (1.2.840.113549.1.1.1)	基本領域の Signature アルゴリズムは以下の通りとする。 sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) 基本領域の subjectPublicKeyInfo アルゴリズムは以下の通りとする。 RSAEncryption (1.2.840.113549.1.1.1)
表 7.1.1 証明書のプロファイル（基本領域）	（項目なし）	項目欄「Subject」に「OrganizationUnitName」をオプション項目として 1 つ追加。 説明：認証局で採番するユニーク ID 記載することができる。
表 7.1.1 証明書のプロファイル（基本領域）	項目欄「Subject」の「OrganizationName」「OrganizationUnitName」の説明欄 加入者となる医療機関等が運営団	項目欄「Subject」の「OrganizationName」「OrganizationUnitName」の説明欄 加入者となる医療機関等が運営団体に

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	体に所属している場合は必須。その場合は所属する運営団体の名称運営団体名をローマ字あるいは英語名で OrganizationName に記載し、OrganizationUnitName に医療福祉機関の種類を格納する。	所属している場合は必須。その場合は所属する運営団体の名称運営団体名をローマ字あるいは英語名で OrganizationName に記載し、OrganizationUnitName に表 7.1.3 で定義する保健医療福祉機関等の種類を格納する。
表 7.1.2 証明書のプロファイル（拡張領域 Extensions）	項目欄「KeyUsage」の「KeyEncipherment」 設定しない	項目欄「KeyUsage」の「KeyEncipherment」 オプション項目に変更
7.1.10　保健医療福祉分野の属性（hcRole） 表 7.1.3 HPKI 組織名テーブル（codeData FreeText の定義）	保険医療機関と保険薬局の 2 つが定められている。	以下の 3 項目を追加。 ・介護事業者 （ ‘insurance nursing care facility’） ・地域医療情報連携ネットワーク事業主体 （‘regional medical information network service provider’） ・医療情報共有サービスを提供する民間事業者 （ ‘medical information service provider’）
9.6.4　検証者の表明保障	２．証明書記載事項の確認責任 検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。 ・証明書の署名が正しいこと ・証明書の有効期限が切れていないこと ・証明書が失効していないこと ・証明書の記載事項が、本 CP「7　証明書及び失効リスト及	２．証明書記載事項の確認責任 検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。 ・証明書の署名が正しいこと ・証明書の有効期限が切れていないこと ・証明書が失効していないこと ・証明書の記載事項が、本 CP「7 証明書及び失効リスト及び OCSP

ポリシ項番	現版証明書ポリシ	本事業による改定（案）
	び OCSP のプロファイル」に記述されているプロファイルと合致していること。特に、次の 2 点の検証を実施することは HPKI 認証用証明書として重要である。 - OID 及び Issuer の CN が HPKI の規定に一致していること - hcRole 及び keyUsage の DigitalSignature のみが有効と設定されていること	のプロファイル」に記述されているプロファイルと合致していること。特に、次の 2 点の検証を実施することは HPKI 認証用証明書として重要である。 - OID 及び Issuer の CN が HPKI の規定に一致していること - hcRole 及び keyUsage の DigitalSignature が有効と設定されていること

3.8. モバイル端末からのアクセス時の機関認証方法

全国保健医療情報ネットワークにモバイル端末で接続することは、「医療情報システムの安全管理に関するガイドライン」に準拠した運用方法であれば、原則問題ないと考えられる。しかしながら全国保健医療情報ネットワークに接続し医療情報を提供するサービス事業者が、モバイル端末からの利用可否を判断する立場にあると考えられるため、利用可否を判断するための運用方法を検討する必要があると考える。この運用方法については、モバイル端末での接続サービスを提供するネットワーク事業者に対する要求事項となる可能性がある。このため、以降ではモバイル端末の利用可否のケースと利用可否を制御する運用方法について検討する。

（１）モバイル端末の利用可否のケースの検討

モバイル端末の利用可否について、サービス事業者の運用ポリシにより以下の 3 ケースに分類されると考えられる。

1) モバイル端末の利用を許可しないケース

医療保険のオンライン資格即時確認やレセプトのオンライン請求の場合は、サービス事業者のポリシにより、接続機関は施設からのみのアクセスを求められ、施設外からのモバイル端末を利用したアクセスは禁止されることが想定される。

2) 一部機能でモバイル端末の利用を許可するケース

電子処方箋 ASP サービスのように接続機関が利用する機能によってモバイル端末の利用が制限されることが想定される。この場合は、サービス事業者のポリシにより、電子処方箋アップロード機能については施設外からのモバイル端末を利用したアクセスは許可され、電子処方箋ダウンロード機能については施設外からのモバイル端末を利用したアクセスは禁止されることが想定される。

3) モバイル端末の利用を許可するケース

電子カルテ共用サービスや医療情報配信サービス等の場合は、サービス事業者のポリシにより、接続機関は施設からのアクセスでも、施設外からのモバイル端末を利用したアクセスでも、許可されることが想定される。

以上の 3 ケースのサービス例を図表 3-22 に示す。

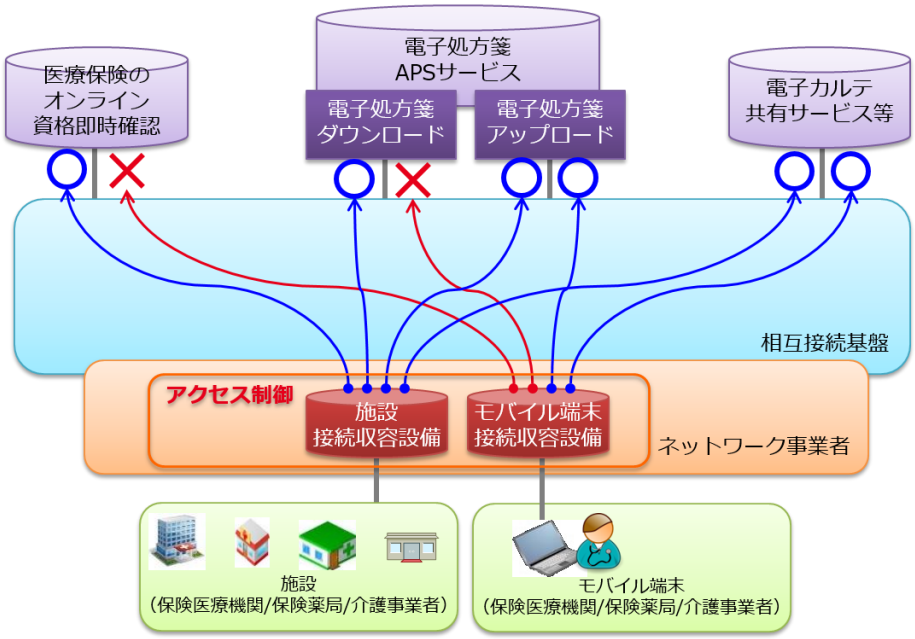
図表 3-22 モバイル端末利用のサービス例

分類	モバイル端末利用ポリシ	サービス例		利用者／利用施設例	モバイル端末利用可否
1)	不可	医療保険のオンライン資格即時確認		保険医療機関（施設） 保険薬局（施設）	×
2)	一部可	電子処方箋 APS サービス	電子処方箋アップロード	保険医（人）	○
			電子処方箋ダウンロード	保険薬局（施設）	×
3)	可	電子カルテ共有サービス等		医師（人） 歯科医師（人） 保険医療機関（施設）	○

（２）接続可否を制御する運用方法の検討

全国保健医療情報ネットワーク内において、サービス事業者にアクセスした段階においては、アクセス元の接続機関がモバイル端末で接続したか否かを判定することはできない。このため、全国保健医療情報ネットワークに接続する段階で、具体的にはネットワーク事業者のゲートウェイにおいて、アクセス元の接続機関がモバイル端末で接続したか否かを判定し適切にアクセス制御を実施する運用方法が考えられる。この運用方法における接続イメージを図表 3-23 に示す。

図表 3-23 モバイル端末のアクセス制御イメージ



3.9. クラウドサービスとの接続時の機関認証方法

クラウドサービスとはクラウドサービス事業者が提供するサービスであり、サービス事業者の 1 つの形態と考えることができる。従ってクラウドサービス事業者のセキュリティ基準及び審査方法についても、本事業で提示するサービス事業者と同様の考え方に沿って検討する。

（1）クラウドサービスのセキュリティ基準

クラウドサービス事業者の場合も、サービス事業者と同様に以下に示す三省 4 ガイドラインを準拠する必要があると考えられる。

1) 医療情報システムの安全管理に関するガイドライン第 5 版（以下、参考文献(5)）
2) ASP・SaaS における情報セキュリティ対策ガイドライン（以下、参考文献(6)）
3) ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン第 1.1 版（以下、参考文献(7)）
4) 医療情報を受託管理する情報処理事業者向けガイドライン第 2 版（以下、参考文献(8)）

しかしながら上記のガイドラインはクラウドサービスを想定したものではないため、そのままセキュリティ基準とすることは難しい。特に図表 3-24 に示す留意点及び確認事項があると考える。

図表 3-24 クラウドサービスでの留意点と確認事項

留意事項	確認事項
一般に所在が明確でない	・ 当該サービスが日本国内法の適用が可能かどうか、設置場所、他国の法の影響等の確認が必要である。 ・ 保健医療データが他のサービス（全国保健医療情報ネットワークとは別のネットワークで接続可能なサービス）と共用エリア・共用ストレージに処理・保管されていないかどうか、処理・保管されている場合は物理的または論理的に分離されているかどうかの確認が必要である。
一般にインターネット接続が前提のサービスが多い	・ 接続認定要件を受けたネットワーク事業者を使用すれば問題ないが、独自にネットワーク接続する場合は、そのネットワークについてガイドラインに準拠しているかどうかの確認が必要である

以上のことから、「クラウドサービス提供における情報セキュリティ対策ガイドライ

ン」（以下、参考文献(9)）をベースに、ASP・SaaS 事業者の場合と同様に、クラウドサービス事業者を対象とした医療情報を取り扱う際の安全管理に関するセキュリティ基準ガイドラインの策定が必要であり、同ガイドラインをセキュリティ基準とすることが考えられる。

（２）クラウドサービスのセキュリティ基準の審査方法

クラウドサービス事業者の場合も、他のサービス事業者と同様に「第三者評価機関の調査を受けて得た認定または適合性評価」等の結果を申告することで、準拠性を立証する必要がある。しかしながら、現在、クラウドサービス事業者を対象としたセキュリティ基準となるガイドラインが存在しないため、その適合性評価及び実施する第三者評価機関が存在しない。

以上のことから、クラウドサービス事業者の審査を実施するためには、クラウドサービス事業者を対象としたガイドラインの適合性評価及び実施する第三者評価機関の整備が必要である。

（３）調査結果のまとめ

クラウドサービス事業者を対象とした医療情報を取り扱う際の安全管理に関するガイドラインの策定、同ガイドラインの適合性評価及び実施する第三者評価機関を整備することにより、本事業の「セキュリティ規定（接続機関向け）」に沿って審査することが可能となると考えられる。

3.10. 証明書を使用した利用者認証システム構築の留意事項

本事業にて検討した証明書プロファイルに対して、「JAHIS HPKI 電子認証ガイドライン V1.1」（以下、参考文献(10)）を参考に認証方法を調査した。認証方法について図表 3-25 に示すケースを想定して検討した。

図表 3-25 認証方法の想定ケース

想定ケース	検討内容
機関認証用証明書をネットワークレベルに用いた「VPN センターVPN ルータ／VPN ソフト」間における認証方法	接続機関とネットワーク事業者とは、IPsec+IKE 方式のインターネット VPN で接続することを想定し、VPN センタと VPN ルータ／VPN ソフトとの間での機関認証用証明書の使用方法を検討する。
機関認証用証明書をアプリケーションレベルに用いた「WEB サーバークライアント端末」間における認証方法	接続機関内のクライアント端末と接続機関内 WEB サーバとは、TLS1.2 を用いた HTTPS で接続することを想定し、WEB サーバとクライアント端末との間での機関認証用証明書の使用方法を検討する。

（1）PKI 認証における留意事項

PKI 認証とは、機関認証用証明書の私有鍵と公開鍵証明書により電子認証を行う仕組みのことである。私有鍵による署名を検証することにより本人性を確認し、公開鍵証明書の検証によって実在性を確認することで、機関認証用証明書所有者を認証することができる。PKI 認証を実装する場合の方法には様々な方式があるが、想定ケースに対する VPN センタ及び WEB サーバの実装要件案を図表 3-26 に示す。

図表 3-26 VPN センタ及び WEB サーバの実装要件案[14]

項目	内容	要求レベル	
		VPN センタ	WEB サーバ
トラストアンカの適切な設定と管理	トラストアンカとして機関認証用ルート認証局が設定できること。 トラストアンカの設定を安全に管理すること。	必須	必須
機関認証用証明書の公開鍵を用いた署名	機関認証用証明書の公開鍵を用いて、クライアントから送られてきた機関認証用証明書の秘密鍵による署名を検証すること。	必須	必須

[14]出典：「JAHIS HPKI 電子認証ガイドライン V1.1」中、「7.4 サーバの実装要件」を参考に作成。

項目	内容	要求レベル	
		VPN センタ	WEB サーバ
の検証			
機関認証用証明書の認証パスの有効性確認	機関認証用証明書からトラストアンカとなる機関認証用ルート認証局までの認証パスを検証できること。 検証方法は RFC5280 のパス検証に従う。 代表的な検証項目として以下のものがある。 ・機関認証用証明書からトラストアンカまでのパス構築 ・機関認証用証明書に付与された認証局の署名の検証 ・認証局証明書の CA フラグの確認 ・証明書ポリシの確認 ・証明書の鍵使用目的の確認 ・認証パス上の証明書の有効期間確認 ・認証パス上の証明書の失効確認 ・失効情報に付与された署名の検証	必須	必須
SubjectName 属性の取得	機関認証用証明書から SubjectName 属性の取得を取得する。	オプション	オプション
hcRole 属性の取得	機関認証用証明書から hcRole 属性の取得を取得する。	オプション	オプション

（２）その他の留意事項

その他の留意事項として、PKI 認証以外の実装要件案を以下に示す。

1) 機関用 OID を用いたアクセス制御

ネットワーク事業者及びサービス事業者において、接続機関を個々に確認してアクセス制御を行う場合には、機関認証用証明書の Subject-OrganizationUnitName に設定された機関用 OID の確認によるアクセス制御が考えられる。

2) hcRole を用いたアクセス制御

ネットワーク事業者及びサービス事業者において、接続機関の資格属性（保険医療機関や保険薬局、介護事業者等）を確認してアクセス制御を行う場合には、機関認証用証明書の subjectDirectoryAttributes に設定された hcRole 属性の確認によるアクセス制御が考えられる。また、subjectDirectoryAttributes が機器の実装上確認できない場合は、Subject-OrganizationUnitName に設定された hcRole 属性が代替とできる。

3)　接続する機器情報によるアクセス制御

サービス事業者において、接続する機器（VPN ルータ、或いは VPN ソフトが導入されたモバイル端末等）を判別して適切なアクセス制御を要求する場合には、本報告書「3.8.（２）接続可否を制御する運用方法の検討」に示すような、ネットワーク事業者のゲートウェイが接続する機器を判定して適切にアクセス制御を行う方式が考えられる。

4)　追加認証によるアクセス制御

サービス事業者において、接続機関（組織）の認証に加え有資格者（人）の認証のうえで適切なアクセス制御を実施する場合には、機関認証用証明書での PKI 認証に、HPKI 人認証用証明書による PKI 認証や ID・パスワード認証等と組み合わせる方式が考えられる。

5)　機関用 OID を用いたログ追跡

障害対応やセキュリティ事故対応において、ネットワーク事業者及びサービス事業者のアクセスログを紐付けする場合には、各事業者のアクセスログに機関用 OID を記録しておくことで、アクセスログの紐付けやログ追跡が容易となる。

（３）外部利用者認証システムについての考察

全国保健医療情報ネットワークにおいて、外部利用者認証システム（以下、認証オーソリティ）を構築し、SAML（Security Assertion Markup Language）等の認証連携のフレームワークを用いることで、WEB サーバ（アプリケーション）から PKI 認証の機能を独立させることができる。SAML の仕組みは固有の認証方法には依存していないため、様々な認証方法を採用することができる。PKI 認証による接続機関の認証を行う場合には、認証オーソリティが接続機関の機関認証用証明書を検証する。

PKI 認証を使用した事例については日本医師会が認証サーバを構築・運用しており、「経済産業省　平成 22 年度　サービス産業活動環境整備調査事業（医療等情報化共通基盤構築調査事業）『成果報告書』及び『添付資料 SAML 実装仕様書』」（以下、参考文献(11)）が参考となる。また、構築や実装については「JAHIS『シングルサインオン実装ガイド』及び『JAHIS シングルサインオンにおけるセキュリティガイドライン Ver.1.0』」（以下、参考文献(12)）が参考となる。

SAML では認証オーソリティが接続機関の認証を行い、その結果を含めた認証アサーションを発行する。WEB サーバ（アプリケーション）は認証オーソリティから認証アサーションを取得することにより、接続機関の本人性や実在性を確認することができる。この仕組みを利用することでシングルサインオンや、異なるドメイン間の ID 連携を実現することが可能となる。

3.11. IPsec-VPN、SSL-VPN、Open-VPN 等の暗号化ネットワークに影響ない証明書を利用した認証運用の方式

本項では、暗号化ネットワークに影響ない証明書を利用した認証運用の方式について検討した。調査過程において、SSL-VPN は一般名称であり、製品により実装方法が様々であることが判明した。また Open-VPN は SSL-VPN の一種と考えることができることが判明した。このため、以降では「IPsec-VPN」と「Open-VPN（SSL-VPN の一種)」を対象に調査した。

（1）IPsec-VPN と Open-VPN の調査

調査対象の方式に対して、機能、実装、セキュリティ、運用の観点から調査した。調査結果を図表 3-27 に示す。

図表 3-27 IPsec-VPN と Open-VPN の調査結果

調査内容		調査結果	
		IPsec-VPN	Open-VPN
機能性		暗号強度・暗号化対象レイヤ（L3）の差異はない。大きな違いは下記 2 点である。	
	認証・鍵共有プロトコル	IKEv2	TLS1.2
	データ暗号化プロトコル	IPsec	IPsec ベースの独自実装
プロトコルの評価		IKEv2・IPsec	TLS1.2・IPsec ベースの独自実装
	安全性	現時点で脆弱性の報告はなく安全である。	現時点で脆弱性の報告はなく安全である。
	安定性	直近で脆弱性報告は少なく枯れており安定している。	TLS1.2 は過去バージョンにおいて脆弱性報告が多く TSL1.3 の規格化も進行中であり、安定性に欠ける。IPsec ベースの独自実装部分は安定性の評価が難しい。
サービス提供を行うネットワーク事業者が存在するか		「支払基金等へのレセプトオンライン請求用 IPsec＋IKE サービス」等のサービスを提供するネットワーク事業者が存在する。	現状、サービス提供を行うネットワーク事業者が存在せず、利用者自身の責任において利用する。
第三者評価機関による評価		HISPRO による「支払基	現状、評価ができる第三

調査内容	調査結果	
	IPsec-VPN	Open-VPN
が可能かどうか	金等へのレセプトオンライン請求用 IPsec＋IKE サービス」の適合性評価がある。	者評価機関が国内には存在しない。

（２）IPsec-VPN の調査結果のまとめ

IPsec-VPN に関しては、ネットワーク事業者にてサービス提供している実績があること、ガイドラインへの適合性を HISPRO 等の第三者評価機関にて評価でき安全なネットワークであることの証明ができること等から、全国保健医療情報ネットワークへの接続方式に適用できると考える。

（３）Open-VPN の調査結果のまとめ

Open-VPN に関しては、機能性においては IPsec-VPN との大きな差異はなかったが、ネットワーク事業者にてサービス提供している実績がないこと、ガイドラインへの適合性を評価する第三者評価機関が存在せず安全なネットワークであることの証明ができないこと等から、全国保健医療情報ネットワークへの接続方式に適用できないと考える。

しかしながら、今後、Open-VPN でのネットワーク事業者によるサービス提供や、第三者評価機関によるガイドライン適合性評価が実現すれば、全国保健医療情報ネットワークへの接続方式としての適用は検討可能であると考える。

3.12. 接続機関の規定

本項では、接続機関向けの規定について素案作成のための調査を行った。調査対象とした規定は図表 3-28 の通りである。

図表 3-28 接続機関の規定

規定名称	内容
セキュリティ規定	全国保健医療情報ネットワークに接続するために機関認証主体が審査する際のセキュリティ基準
接続規定	全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式

3.12.1. セキュリティ規定

本項では、接続機関が全国保健医療情報ネットワークに接続するために機関認証主体が審査する際のセキュリティ基準について考察する。

（１）調査の対象

調査対象とする接続機関は以下とする。

- 保険医療機関
- 保険薬局
- 介護事業者
- 地連事業主体
- サービス事業者

（２）調査にあたっての留意事項

接続機関の区分とは別に全国保健医療情報ネットワークでは、リクエスタ、レスポンダ、といった役割が存在し、その役割に応じてセキュリティ基準の考え方が異なることが想定されるため、調査に際して注意が必要である。図表 3-29 にリクエスタ、レスポンダについて定義する。

図表 3-29 接続機関の役割の定義

役割	定義
リクエスタ	・ 全国保健医療情報ネットワークを介して医療情報を参照する接続機関
レスポンダ	・ 全国保健医療情報ネットワークを介して医療情報を提供する接続機関 ・ 全国保健医療情報ネットワークの DNS に IP アドレスが登録される ・ リクエスタを兼ねる場合がある

（3）セキュリティ基準の考察

全国保健医療情報ネットワークは、医療情報を取り扱うネットワーク・システム基盤であることから、接続機関に求めるセキュリティ基準は図表 3-30 に示す三省 4 ガイドラインに準拠していることと考えることができる。

図表 3-30 三省 4 ガイドライン

対象者	ガイドライン名	所管
医療機関サイド	医療情報システムの安全管理に関するガイドライン	厚生労働省
受託事業者サイド	ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン	総務省
	ASP・SaaS における情報セキュリティ対策ガイドライン	総務省
	医療情報を受託管理する情報処理事業者向けガイドライン	経済産業省

三省 4 ガイドラインのうち準拠すべきガイドラインは、接続機関及び役割（リクエスタ／レスポンダ）により異なるため、接続機関及び役割に応じたセキュリティ基準が必要である。

（4）セキュリティ基準の結論

接続機関は、三省 4 ガイドラインを準拠することが求められる。また、接続機関の役割（リクエスタ／レスポンダ）に応じて準拠すべき範囲が異なる。接続機関が役割に応じて準拠すべきガイドラインの対象範囲を図表 3-31 に示す。なお、リクエスタとしての地連事業主体及びサービス事業者は対象外とした。

図表 3-31 接続機関及び役割に応じて対象範囲となるガイドライン

役割	接続機関	＜厚生労働省＞医療情報システムの安全管理に関するガイドライン	＜総務省＞ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン	＜総務省＞ASP・SaaS における情報セキュリティ対策ガイドライン	＜経済産業省>医療情報を受託管理する情報処理事業者向けガイドライン
リクエスタ	保険医療機関	○	―	―	―
	保険薬局	○	―	―	―
	介護事業者	○	―	―	―
	地連事業主体				
	サービス事業者				
レスポンダ（兼リクエスタ）	保険医療機関（情報提供を行っている中核病院等）	○	○	○	△
	保険薬局（存在する場合）	○	○	○	△
	介護事業者（存在する場合）	○	○	○	△
	地連事業主体	○	○	○	△
	サービス事業者	○	○	○	△

○：対象、△：場合により対象、－：対象外

（５）セキュリティ基準の審査方法の考察

機関認証主体における、接続機関のセキュリティ基準の準拠性の審査方法は、認証局で実施する方法を踏襲し以下とすることが考えられる。

- 審査方法：接続機関は、機関認証主体にガイドラインの準拠性を立証し、機関認証主体はそれを確認する。

セキュリティ基準の準拠性を審査する方法としては 4 つの案が考えられる。各々の案に関してメリット・デメリットを図表 3-32 に示す。

図表 3-32 セキュリティ基準の審査方法のメリット・デメリット

案	審査方法（案）	メリット	デメリット
A	【直接確認】 接続機関は、機関認証主体の現地調査等を受けて、準拠性を立証する	・信頼性が高い	・機関認証主体に専門知識が必要 ・機関認証主体に調査体制が必要 ・接続機関の負荷-高 ・実施が困難
B	【自己申告】 接続機関は、「準拠性チェックシート」等の自己チェック結果を申告することで、準拠性を立証する	・機関認証主体の負荷-低 ・接続機関の負荷-低 ・実施が容易	・客観的な申告とならないおそれがあり信頼性が低い ・「準拠性チェックシート」等の策定が必要（課題 1）
C	【第三者評価】 接続機関は、「第三者評価機関の調査を受けて得た認定または適合性評価」等の結果を申告することで、準拠性を立証する	・信頼性が高い ・機関認証主体の負荷-低	・接続機関の負荷-高 ・該当する第三者評価機関があまり存在しない（課題 2）
D	【既存資格による確認】 接続機関は、「既に業務上の責務として実施している第三者評価機関による監査」等の結果を申告することで、準拠性を立証する	・機関認証主体の負荷-低 ・接続機関の負荷-低	信頼性が実施している監査等の内容に依存する（課題 3）

上記の表で考察した課題に関しては、図表 3-33 の対応案が考えられる。

図表 3-33 セキュリティ基準の審査方法の課題と対応（案）

課題	対応（案）
課題 1	知見を有する第三者評価機関に「準拠性チェックシート」等の策定を依頼する。第三者評価機関として HISPRO が候補の一つとして挙げられる。
課題 2	第三者評価機関に「全国保健医療情報ネットワークに対応した適合性評

課題	対応（案）
	価制度」等の制度新設を依頼する。第三者評価機関として HISPRO が候補の一つとして挙げられる。
課題 3	現在医療機関等が受けている指導・監査等の内容が正確に把握できないため、信頼性の評価ができない。このため案 D は検討外とする。

（６）セキュリティ基準の審査方法の結論

接続機関の役割に応じた審査方法の結論及び選定理由を図表 3-34、図表 3-35 に示す。

図表 3-34 リクエスタの場合の審査方法

接続機関	・ 保険医療機関 ・ 保険薬局 ・ 介護事業者
審査方法	案 B【自己申告】とする。 ・ 接続機関は、「準拠性チェックシート」等の自己チェック結果を申告することで、準拠性を立証する
選定理由	・ 接続機関が多い（全国に医科 9.4 万、歯科 6.9 万、薬局 5.7 万、介護施設 17 万）ため、自己申告以外の準拠性確認を実施することは現実的ではない。 ・ 準拠すべきガイドラインは「医療情報システムの安全管理に関するガイドライン」に限定される。 ・ 保険医療機関、保険薬局、介護事業者は、その業務を遂行するうえで、ガイドラインを準拠する義務があり、また所管（国、自治体等）から「指導・監査」を受けている。 ・ リクエスタの場合、セキュリティ事故発生時の影響範囲は当該施設に限られるケースが想定される。

図表 3-35 レスポンダの場合の審査方法

接続機関	・ 保険医療機関 ・ 保険薬局 ・ 介護事業者 ・ 地連事業主体 ・ サービス事業者
審査方法	案 C【第三者評価】とする。 ・ 接続機関は、「第三者評価機関の調査を受けて得た認定または適合性評価」等の結果を申告することで、準拠性を立証する
選定理由	・ 準拠すべきガイドラインは三省 4 ガイドラインほぼ全てである。 ・ レスポンダの場合、セキュリティ事故発生時の影響範囲が広範囲となるケースが想定される。 ・ 下記のような第三者評価機関による評価制度が存在し現実的に実施可能であると考えられる。 例）HISPRO の適合性評価 -「支払基金等へのレセプトオンライン請求用 IPsec＋IKE サービス」 -「民間事業者による医療情報の外部保存及び ASP・SaaS サービス」

（7）セキュリティ基準の審査方法の課題

レスポンダに対するセキュリティ基準の審査方法として、セキュリティの信頼性といった点においては第三者評価機関による適合性評価は妥当と考える。しかし、コストの点においては特に地連事業主体や地域の中核病院の参入の妨げになることが考えられ、審査方法の精緻化が必要と考える。「第三者評価」よりは安価で「自己申告」よりは信頼性を高める対応案として、例えば地連事業主体や地域の中核病院の場合には、ホームページ等で「準拠性チェックシート」の自己チェック結果を他の接続機関に公開することを前提に、機関認証主体では自己申告にて審査を行う方法等が考えられる。

3.12.2. 接続規定

本項では、接続機関が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式について考察する。

（１）調査の対象

調査対象とする接続機関は以下とする。

- 保険医療機関
- 保険薬局
- 介護事業者
- 地連事業主体
- サービス事業者

（２）ネットワーク接続方式の要件

全国保健医療情報ネットワークに接続するためのネットワーク接続方式の要件は以下が考えられる。

- 全国保健医療情報ネットワークは医療情報を取り扱うネットワークであることから、「医療情報システムの安全管理に関するガイドライン」に準拠していることが必要と考える。
- ネットワーク層の接続方式であることから、「オブジェクト・セキュリティ」は対象外とし、「チャネル・セキュリティ」を検討する。
- 現実的に提供可能であることが必要である。

（３）ネットワーク接続方式の考察

全国保健医療情報ネットワークに接続するためのネットワーク接続方式として選択可能なものを、図表 3-36 の「医療情報システムの安全管理に関するガイドライン」の「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の「B-2. 選択すべきネットワークのセキュリティの考え方」に記載されている方式から考察する。

図表 3-36 ネットワーク接続方式の考察対象

形態	方式
クローズドなネットワークで接続する場合	専用線
	公衆網（ISDN／ダイアルアップ接続等）
	閉域 IP 通信網（IP-VPN）
オープンなネットワークで接続されている場合	SSL-VPN（5 階層目の「セッション層」といわれる部分で経路の暗号化手続）
	IPsec（2 階層目もしくは 3 階層目の「ネットワーク層」といわれる部分より下位の層で経路の暗号化手続）
	TLS1.2（HTTP に限定）

選択可能なネットワーク接続方式の考察結果を図表 3-37 に示す。

図表 3-37 ネットワーク接続方式の考察結果

形態	方式	ガイドラインに準拠しているか	現実的に提供可能か	推奨
クローズドなネットワーク	専用線	準拠している	場合により可 ・品質は高いが比較的高価である。地連事業主体やサービス事業者であれば選択肢となりえる。	△
	公衆網（ISDN／ダイアルアップ接続等）	準拠している	不可 ・今後サービスは終了していく傾向にある。	×
	閉域 IP 通信網（IP-VPN）	準拠している	可 ・ネットワークサービスが比較的安価に提供されている。	○
オープンなネットワーク	SSL-VPN	準拠していない ・ガイドラインにて「原則使用すべきではない」ネットワークとされている。理由は以下の通り。 1) 正しく経路が暗号化されれば問題ないが、経	不可 ・ガイドラインへの適合性を評価する第三者評価機関がないため安全かどうかの判断ができない。 ・適合性評価を受けたネットワークサービスが存在	×

形態	方式	ガイドラインに準拠しているか	現実的に提供可能か	推奨
		路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。 2) 偽サーバへの対策が不十分なものが多い。	しない。	
	IPsec	準拠している ・IKE で暗号化鍵の交換を実施することが条件となる。	可 ・ガイドラインへの適合性を評価する第三者評価機関がある。 ・適合性評価を受けたネットワークサービスが比較的安価に提供されている。	○
	TLS1.2	対象外 ・ネットワーク層のセキュリティ対策ではない。	対象外 ・ネットワーク層のセキュリティ対策ではない。	対象外

○：推奨、△：場合により推奨、×：非推奨

（4）ネットワーク接続方式の結論

全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式としては、接続機関ごとのネットワーク接続方式は図表 3-38 を推奨し、どの方式を採用するかは接続機関の判断に委ねる。いずれの方式も全国保健医療情報ネットワークの事業主体が認めたネットワーク事業者から提供するサービスであることが条件となる。

図表 3-38 接続機関が選択可能なネットワーク接続方式

接続機関	選択可能なネットワーク接続方式
・ 保険医療機関 ・ 保険薬局 ・ 介護事業者	・ IP-VPN 接続サービス ・ インターネット VPN（IPsec+IKE）接続サービス
・ 地連事業主体 ・ サービス事業者	・ IP-VPN 接続サービス ・ インターネット VPN（IPsec+IKE）接続サービス ・ 専用線接続サービス

なお、本事業において選択可能としていない他のネットワーク接続方式に関して

も、最新の「医療情報システムの安全管理に関するガイドライン（厚生労働省）」に適合し、かつ、相互接続基盤の事業主体が認めるネットワーク接続方式であれば、今後選択可能になることが想定される。

（５）ネットワーク認証での機関認証用証明書の利用について

全国保健医療情報ネットワークに接続するネットワーク接続方式において、機関認証主体より発行する機関認証用証明書を、ネットワーク事業者がネットワーク認証に使用することが考えられる。この機関認証用証明書のネットワーク事業者の利用を必須とした場合（ネットワーク認証には機関認証用証明書のみ利用できる場合）と任意とした場合（ネットワーク認証には機関認証用証明書及び他の証明書が利用できる場合）について、そのメリット・デメリットの考察結果を図表 3-39 に示す。

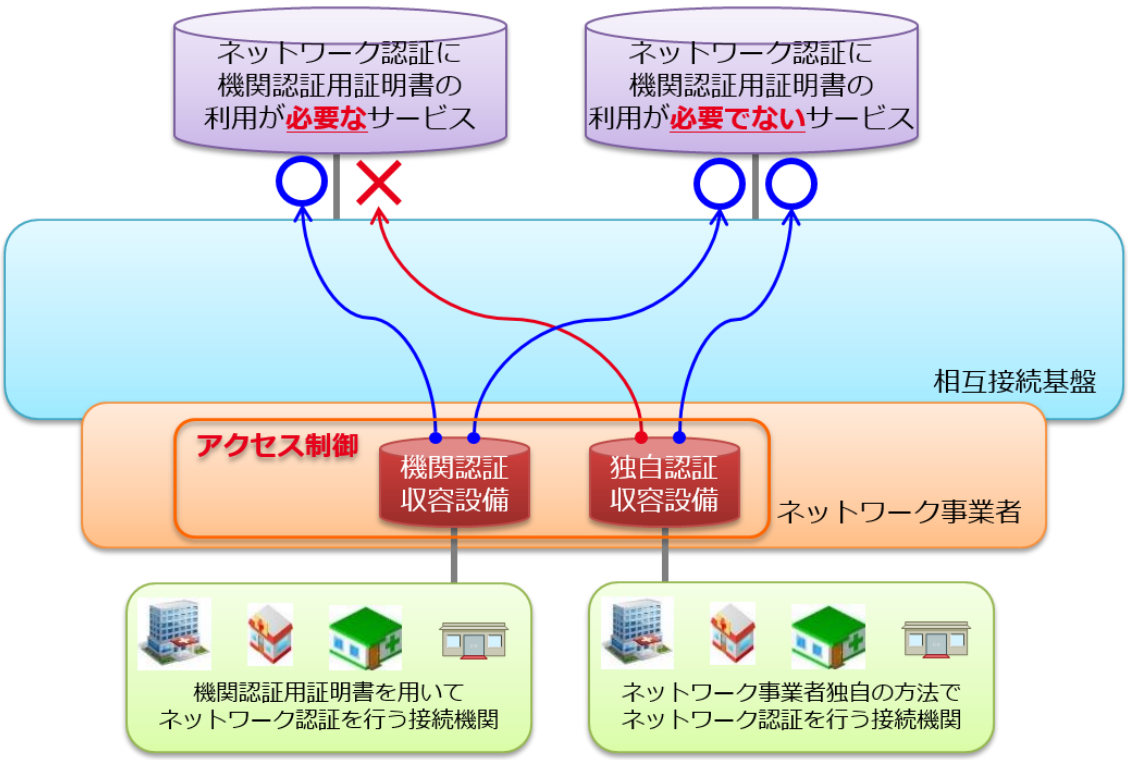
図表 3-39 機関認証用証明書の利用の任意、必須の比較

評価者	必須とした場合	任意とした場合
相互接続基盤の事業主体	・ 接続機関の信頼性が一定になることが期待できる ・ 接続機関の管理が容易になる	・ 接続機関の信頼性にばらつきがでるおそれがある ・ 接続機関を管理しづらくなる
接続機関	・ 他の接続機関の信頼性の確認が容易 ・ 証明書費用の負担がある	・ 他の接続機関の信頼性を確認しづらい ・ 証明書費用の負担がない（ネットワーク事業者による）
ネットワーク事業者	・ 対応のための負担増 ・ 対応できないネットワーク事業者がいるおそれがある ・ 独自証明書の廃止により運用費の削減	・ ネットワーク事業者の判断で対応できる ・ 独自証明書の維持による運用費の増加
その他	・ 既存の地域医療情報連携ネットワークが接続する際の障害となるおそれがある	－

結論としては、現時点では機関認証用証明書をネットワーク事業者が利用するかどうかに関してはネットワーク事業者の判断に委ね、任意とするべきと考える。理由は、将来独自に証明書を必須とするサービスが始まることは想定されるが、現時点は任意として、運用は実状に合わせてネットワーク事業者に任せることが妥当と判断したためである。しかしながら全国保健医療情報ネットワーク内でサービスを提供するサービス事業者のセキュリティポリシーによっては、ネットワーク認証に機関認証用

証明書の利用を必要とするサービスと、必要としないサービスが混在することが想定される。実現案としては図表 3-40 図表 3-40 に示すような、ネットワーク事業者のゲートウェイで機関認証用証明書を利用した接続か否かを判定し適切にアクセス制御する方式等が考えられるが、今後検討していく必要があると考える。

図表 3-40 ネットワーク認証でのアクセス制御イメージ



4. ネットワーク接続事業者の接続規定

ネットワーク事業者に関する以下のドキュメント素案を作成することを目的とし、ネットワーク事業者が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式、接続認定のためのセキュリティ基準、運用要件等について検討した。

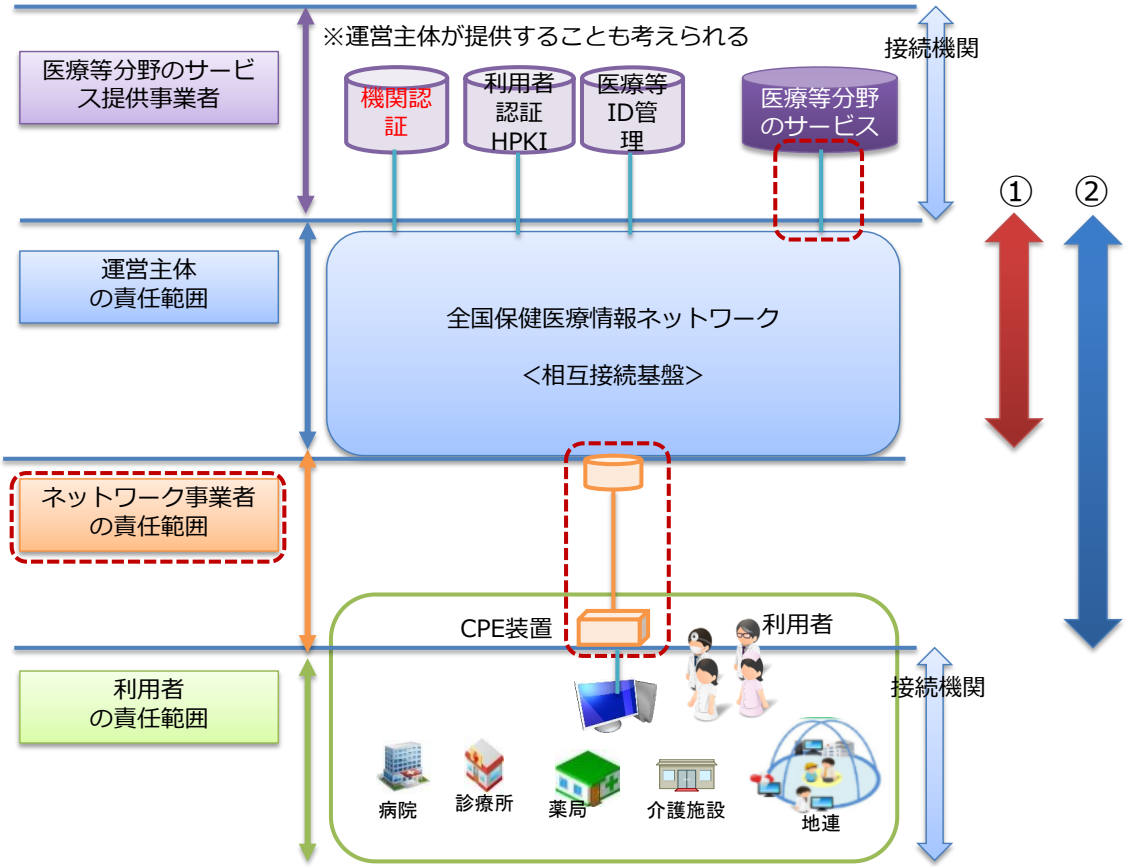
図表 4-1　ネットワーク事業者の規定

規定名称	内容
接続規定	ネットワーク事業者が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式
接続認定要件	全国保健医療情報ネットワークに接続する際に遵守すべきセキュリティ基準
運用ガイドライン	全国保健医療情報ネットワークに接続するネットワーク事業者向けの障害時対応、監視方法、利用申請方法等のガイドライン

4.1. ネットワーク事業者の接続規定の調査の検討条件

全国保健医療情報ネットワークに係る通信サービス事業者としては、相互接続基盤のネットワークを提供する通信サービス事業者や、医療機関等の接続機関に VPN サービスを提供する通信サービス事業者、また物理的な回線を提供する通信サービス事業者等、役割が異なる事業者が存在する。本事業においてネットワーク事業者とは、接続機関に VPN サービスを提供する通信サービス事業者と定義し、検討を進めた。以下に本事業におけるネットワーク事業者の検討範囲と今後の検討課題について整理した結果を示す。

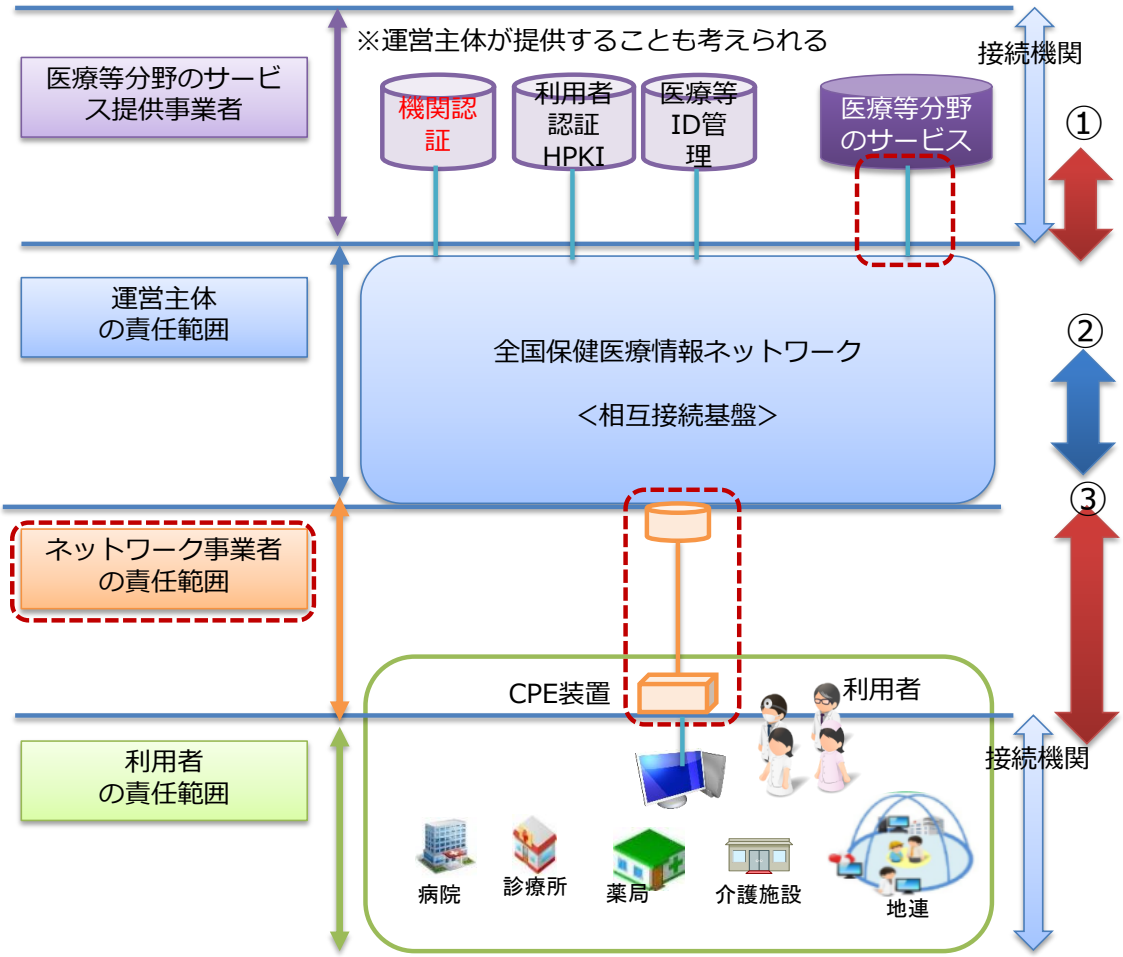
図表 4-2　本事業の対象範囲　（相互接続基盤の事業主体の範囲について）[15]



相互接続基盤の事業主体が責任を持つネットワークの範囲として、図表 4-2 の①相互接続基盤に限定する、②相互接続基盤までの接続サービスを含める（運営主体＋ネットワーク事業者）とする場合が考えられるが、本事業においては、作成すべき規定ドキュメントの位置づけの関係上、①を前提に検討を進めた。②については今後の検討課題として整理する。

[15]出典：総務省実証事業「医療等分野における高精細映像等データ共有基盤の在り方に関する実証の請負」中間報告資料を参考に作成。

図表 4-3　本事業の対象範囲　（ネットワーク事業者の範囲について）[16]



本事業におけるネットワーク事業者の範囲として、図表 4-3 の①医療等分野のサービス事業者は、直接専用線等で相互接続基盤に接続する場合もあるが、ネットワーク事業者が VPN サービスをサービス事業者に提供する場合もあるため、ネットワーク事業者の範囲とする。②ネットワーク事業者としては、運営主体の相互接続ネットワークを提供するネットワーク事業者もあり、今後検討が必要な事項ではあるが、運営主体の検討は今後の検討課題と整理していることから、②は今後の検討課題として整理する。③ネットワーク事業者は、相互接続基盤に接続し、接続機関に VPN サービスを提供するところまでを範囲として検討する。

なお、ネットワーク事業者が VPN サービスを提供する接続機関の対象は、機関認証主体の検討における接続機関と同様に以下の 5 つとする。

[16]出典：総務省実証事業「医療等分野における高精細映像等データ共有基盤の在り方に関する実証の請負」中間報告資料を参考に作成。

1) 保険医療機関
2) 保険薬局
3) 地連事業主体
4) 介護事業者
5) サービス事業者

4.2. 既存ネットワークの接続方式

4.2.1. 全国保健医療情報ネットワークとネットワーク事業者間のネットワーク接続方式

（１）ネットワーク接続方式の要件

ネットワーク事業者が全国保健医療情報ネットワークに接続するためのネットワーク接続方式の要件は下記と考えられる。ただし、全国保健医療情報ネットワークのセキュリティのあり方の検討は本事業の範囲外であるため今後の検討課題と位置づける。

- 全国保健医療情報ネットワークは医療情報を取り扱うネットワークであることから、「医療情報システムの安全管理に関するガイドライン」に準拠していることが必要と考える。
- ネットワーク層の接続方式であることから、「オブジェクト・セキュリティ」は対象外とし、「チャネル・セキュリティ」を検討する。
- 接続機関にサービスとして提供するため、ある程度の性能（帯域、セッション数)、可用性を有していることが望まれる。（例：帯域であれば一般的にブロードバンドと称される 1Gbps または 10Gbps 程度）

（２）ネットワーク接続方式の考察

全国保健医療情報ネットワークに接続するためのネットワーク接続方式として選択可能なものを、図表 4-4 の「医療情報システムの安全管理に関するガイドライン」の「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の「B-2. 選択すべきネットワークのセキュリティの考え方」に記載の方式のうちから考察した。

図表 4-4　ネットワーク接続方式の考察結果

接続方式		NW 事業者の対象（案）
Ⅰ．クローズドなネットワークで接続する場合	専用線	○
	公衆網　（ISDN）	対象外（もう利用されてない）終了している
	閉域 IP 通信　（IP-VPN）	○
Ⅱ．オープンなネットワークで接続されている場合	SSL-VPN　（5 階層目の「セッション層」といわれる部分で経路の暗号化手続がなされる）	対象外（そもそも推奨されてない）
	IPsec（2 階層目もしくは 3 階層目の「ネットワーク層」といわれる部分より下位の層で経路の暗号化手続がなされる）＋ IKE	相互接続基盤がオープンネットワークの接続ぐちを設けるのはセキュリティ対策の観点から現実的でない。
	TLS1.2	
Ⅲ．モバイル端末等を使って医療機関等の外部から接続する場合	1）公衆網（電話網）を経由して直接ダイアルアップする場合	NW 事業者がモバイル端末からアクセスすることはないので対象外である。
	2）インターネットを経由して接続する場合	
	3）閉域ネットワーク（IP-VPN 網）を経由して接続する場合	

（３）ネットワーク接続方式の結論

全国保健医療情報ネットワークとネットワーク事業者の接続方法として、オープンなネットワークで接続できる場合も否定はできないが（全国保健医療情報ネットワークのセキュリティの考え方による)、全国保健医療情報ネットワークのセキュリティ対策の煩雑さを考えると現実的ではない。また、モバイルでの接続はさらに現実的でないことから、クローズドなネットワークで接続することが望ましい。

全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式としては、図表 4-5 を推奨し、どの方式を採用するかはネットワーク事業者の判断に委ねることとする。

図表 4-5　ネットワーク事業者が選択できる接続方式

接続方式	選択可能なネットワーク接続方式
クローズなネットワーク	・　専用線接続 ・　IP-VPN 接続

4.2.2. ネットワーク事業者と接続機関間のネットワーク接続方式

（1）ネットワーク接続方式の結論

接続機関の接続方式は「3.12.2 接続規定」で検討された結果を結論とし、ネットワーク事業者は図表 4-6 のいずれかのネットワークサービスを接続機関に提供できなければならない。

図表 4-6 接続機関が選択可能なネットワーク接続方式　（再掲）

接続機関	選択可能なネットワーク接続方式
・　保険医療機関 ・　保険薬局 ・　介護事業者	・　IP-VPN 接続サービス ・　インターネット VPN（IPsec+IKE）接続サービス
・　地連事業主体 ・　サービス事業者	・　IP-VPN 接続サービス ・　インターネット VPN（IPsec+IKE）接続サービス ・　専用線接続サービス

なお、本事業において選択可能としていない他のネットワーク接続方式に関しても、最新の「医療情報システムの安全管理に関するガイドライン（厚生労働省）」に適合し、かつ、相互接続基盤の事業主体が認めるネットワーク接続方式であれば、今後選択可能になることが想定される。

4.3. 暗号化要件

全国保健医療情報ネットワークとネットワーク事業者が接続するネットワーク接続方式毎に暗号化要件を整理した。

図表 4-7 暗号化要件を含めたネットワークセキュリティ要件

接続方式		セキュリティ
クローズドな NW	専用線	・一般的には暗号化は不要
	IP VPN	・アクセスポイントまでのセキュリティ確保が必要 ・一般的には暗号化は不要
オープンな NW	IPsec+IKE	・IPsec の暗号化方式には「ハイブリッド方式」が採用。実際の通信には速度の速い共通鍵暗号化方式が使われている。 ・IKE で公開鍵暗号化方式を採用

4.4. 接続認定要件

4.4.1. ネットワーク事業者の認定要件

全国保健医療情報ネットワークと接続し、ネットワークサービスを接続機関に提供できるネットワーク事業者を認定する要件を整理した。

（１）組織の実在性

ネットワーク事業者は、接続機関が選択可能なネットワーク接続方式のいずれかを提供できる通信事業者であることが前提である。

1）要件

- 電気通信事業法（昭和 59 年法律第 86 号）第２条第５号に規定する電気通信事業者であること

電気通信事業者は、電気通信回線設備の設置の有無や規模等により、電気通信事業法第９条の登録を受けた者（以下「登録電気通信事業者」という。）と同法第 16 条第１項の規定による届出をした者（以下「届出電気通信事業者」という。）とに分かれている。[17]

2）確認方法

電気通信事業者であることを証明する書類（電気通信事業法第 11 条第２項に規定する通知の写し等）の提出。

登録電気通信事業者については、一覧が総務省のホームページ[18]に掲載されているため、そのページを確認することで、実在性を確認できる。

届出電気通信事業者については、一覧が公開されていないため、確認方法については今後検討が必要である。

（２）組織の申請意思

1）要件

- 申請する組織の責任者が申請をしている

2）確認方法（案）

- 申請書類等への責任者署名・押印の確認

印鑑証明書や登記事項証明書（法人）、住民票（個人のみ）の提出等が必要と思われるが、電気通信事業者の申請時に提出しているため、電気通信事業者であること

---

[17] 総務省、届出電気通信事業者及び登録電気通信事業者とは　（電気通信事業法施行規則第３条第１項）
http://www.soumu.go.jp/soutsu/kanto/com/jigyo/tetuzuki/tetuzuki01.html

[18]参考：（http://www.soumu.go.jp/johotsusintokei/field/tsuushin04.html）

が確認できれば不要である。その他、一般的な商慣習に習うことで確認は十分であると考えられる。

（３）セキュリティ基準準拠の確認

1）要件

医療情報を取り扱う上で一定のセキュリティ基準を満たす必要がある。ネットワーク事業者は三省４ガイドラインのうち厚労省の安全管理ガイドラインを準拠する必要がある。その他のガイドラインについては、サービス事業者にネットワークを提供する観点から内容を把握する必要がある。

相互接続基盤の事業主体が要求するその他のセキュリティ要件については、全国保健医療情報ネットワークのセキュリティのあり方によるところから今後の検討課題とする。

2）確認方法（案）

セキュリティ基準準拠の確認方法としては以下の案が考えられる。

図表 4-8　セキュリティ基準準拠の確認方法

確認方法	確認方法の現状
１．相互接続基盤の事業主体による審査【直接確認】	事業主体で審査できる体制を構築する必要がある。独立した審査体制を作らないと客観性が乏しくなるデメリットもある。
２．外部組織による審査（相互接続基盤の事業主体が認定（信頼）した第三者機関）【第三者確認】	該当する組織があまり存在しない（HISPRO のみ） （例：HISPRO の VPN 事業者向けのレセプトオンライン請求用チェックシートの活用　審査して適合性評価証を授与）※現在のチェックシートが IPsec 用なので、IP－VPN 用も必要
３．チェックシート等による自己審査結果の提出【自己確認】	A)事業主体がチェックシートを作成し、提供 B)事業主体が認定（信頼）した第三者機関が提供する適合評価の結果を提出 実施が容易であるが、自己確認による申請のため信頼性が低い

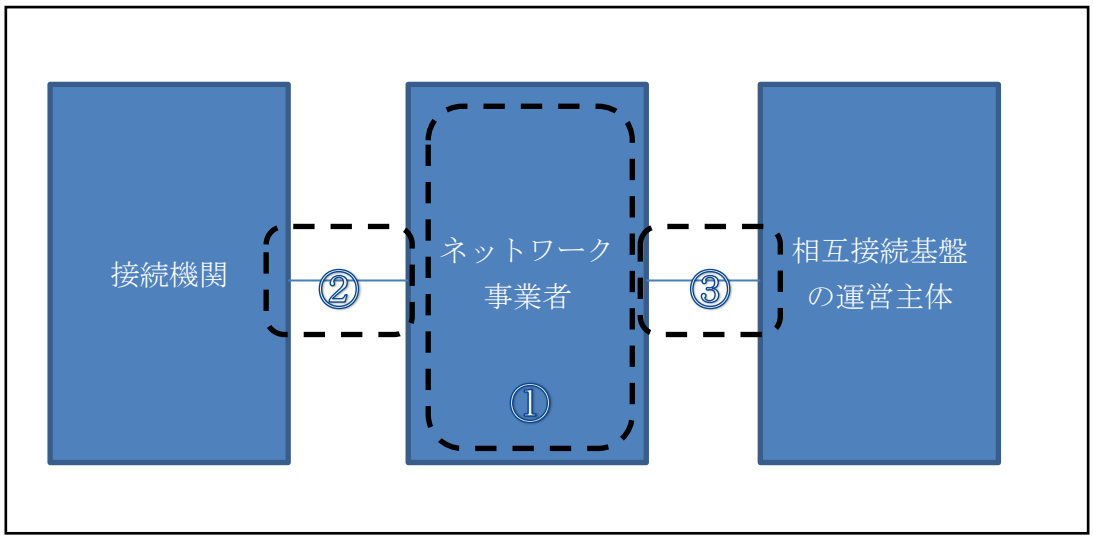
ネットワーク事業者は接続機関にネットワークサービスを提供する事業者であることから審査の基準はある程度高いことが望まれることから、３の自己確認は対象外とし、１及び２がセキュリティ基準準拠の確認方法として適していると考えられる。

4.5. 運用要件

全国保健医療情報ネットワークに接続するネットワーク事業者に求められる運用要件は、「①ネットワーク事業者における運用要件」、「②ネットワーク事業者と接続機関間における運用要件」及び「③ネットワーク事業者と相互接続基盤の事業主体間における運用要件」の 3 つがあると考えられる。

各運用要件の関係を、図表 4-9 に示す。

図表 4-9　ネットワーク事業者に求められる運用要件



これら 3 つの運用要件として規定すべき項目やその内容を検討するにあたり、参考文献(5)、参考文献(6)、参考文献(7)、参考文献(8)のほか、以下に示すドキュメントを参考にした。

1)　チェックリスト項目集（HISPRO 適合性評価）（以下、参考文献(13)）

2)　「厚生労働省 平成 28 年度　医療等分野におけるネットワークの相互接続の実現に向けた調査研究業務報告書」（以下、参考文献(14)）

3)　平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業（平成 27 年 3 月）「運用管理規程」、「緊急時、災害時、障害時の対応手順」（以下、参考文献(15)）

4)　平成 24 年度以降における厚生労働省統合ネットワーク回線・機器に係る供給（設計・開発、テスト、移行及び運用等）業務一式　調達仕様書（以下、参考文献(16)）

5)　電気通信分野における情報セキュリティ確保に係る安全基準（第 3 版）（以下、参考文献(17)）

6)　ネットワークサービスの SLA（サービスレベル合意書）（以下、参考文献(18)）

8)　重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第

5 版）（案）（以下、参考文献(19)）
9)　重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）（案）（以下、参考文献(20)）

運用要件の検討に際しては、本事業で策定する「運用ガイドライン」の記載項目（案）を HEASNET 技術委員会に諮り、項目の過不足等について、レビューを実施した。

レビュー結果として得られた各意見について対応方針を検討し、必要に応じて記載項目（案）の追記や削除を行った。

HEASNET 技術委員会から挙げられた主な意見を、以下に示す。これらは、全て運用ガイドラインの記載項目として反映した。

- ネットワーク機器や証明書の変更や更新に関する手順等が必要
- 通信基盤の冗長化に関する内容が必要
- 障害時等の報告方法について考慮が必要
- 利用規約違反時の対応手順等が必要

4.5.1. ネットワーク事業者における運用要件

「ネットワーク事業者における運用要件」としては、全国保健医療情報ネットワークに接続するネットワーク事業者が、当該ネットワークサービスを運用するにあたって遵守すべき要件を検討した。

具体的には、ネットワークサービス運用の基本方針及び障害時対応について整理した。

また、全国保健医療情報ネットワークに接続するネットワーク事業者は、相互接続基盤の事業主体が定める「接続認定要件」等を満たす必要があるため、ネットワーク事業者が実施する接続申請等の手順についても検討した。

4.5.2. ネットワーク事業者と接続機関間における運用要件

「ネットワーク事業者と接続機関間における運用要件」としては、ネットワーク事業者と接続機関それぞれの立場で、遵守すべき事項を検討した。

具体的には、ネットワーク事業者が遵守すべき事項として、「接続機関との契約締結時におけるサービスレベルの明示」と、「接続機関向けの接続規定のうちネットワークサービスに関する要件の遵守」について規定することとした。なお、接続機関向けの接続規定は、機関認証を取得する接続機関を対象としたドキュメントであるため、機関認証を取得していない接続機関に対しては、当該接続規定とは別に求められるネットワーク要件を満たすことが必要である旨も、明記することとした。

一方、接続機関が遵守すべき事項は、接続機関向けの接続規定及びセキュリティ規定に示されている。そこで、それらの規定を遵守しなかった場合の対応手順として、

相互接続基盤への接続停止に係る手順を検討した。

また、接続機関が行う申請のうち、ネットワーク事業者が関係する手続について、手順を検討した。具体的には、「相互接続基盤の事業主体に対するネットワーク事業者認定の取得」と「ネットワーク事業者に対するネットワーク利用（新規、変更、廃止)」を対象とした。機関認証を取得していない接続機関による申請の場合については、ネットワークサービスの利用開始手続と同時に、機関認証取得申請の必要書類等をネットワーク事業者が受け付け、ネットワーク事業者から機関認証主体に取り次ぐことができるものとして整理した。

さらに、地連事業主体が接続機関としてネットワーク利用申請を行うことを想定した、ネットワーク事業者の責任範囲を整理した。具体的には、ネットワーク事業者が確認するのは「地連事業主体の組織の正当性、ネットワークの安全性の担保」であり、地域医療情報連携ネットワークに接続している医療機関等は地連事業主体が責任を持って確認することとした。

4.5.3. ネットワーク事業者と相互接続基盤の事業主体間における運用要件

本運用要件では、ネットワーク事業者と全国保健医療情報ネットワーにおける運用要件を整理した。

具体的には、ネットワーク監視、障害発生時における報告方法について、検討した。いずれも、相互接続基盤の事業主体が中心となって対応するものであり、ネットワーク事業者は相互接続基盤の事業主体と協力する旨を規定することとした。

5. 接続規定、ガイドラインの策定に向けた調査研究及び素案の作成

5.1. 機関認証主体に関するドキュメント類

認証主体が接続機関に求める認定基準や、認証主体の運用及び機関認証用証明書のライフサイクルについて、調査研究を実施し、この研究結果を踏まえて、認証主体に関する以下のドキュメント素案を作成した。

- 機関認証の証明書ポリシ（保健医療福祉分野 PKI 認証局認証用（組織）証明書ポリシ 1.1 版の改訂版）
- 認証局運用規程（改訂版の HPKI-CP に対応した運用規程）
- 準拠性審査基準（機関認証主体が基準に適合するかを専門家が審査するための基準）
- 事務取扱要領（認証局運用規程を基に、認証局の運用業務内容を詳細に規定）

5.2. 接続機関に関するドキュメント類

接続機関が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式、接続認定のためのセキュリティ基準について、調査研究を実施し、この研究結果を踏まえて、接続機関に関する以下のドキュメント素案を作成した。

- 接続規定　（接続機関が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式）
- セキュリティ規定　（接続機関が全国保健医療情報ネットワークに接続するために機関認証主体が審査する際のセキュリティ基準）

5.3. ネットワーク事業者に関するドキュメント類

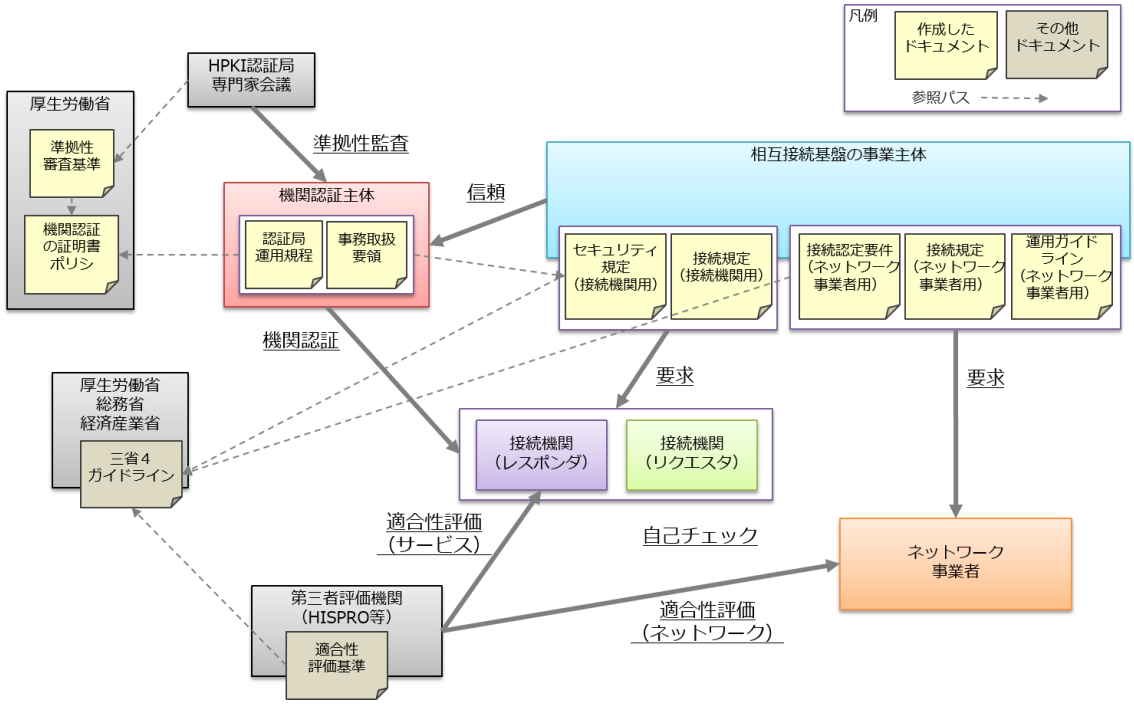
ネットワーク事業者が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式、接続認定のためのセキュリティ基準、運用要件について、調査研究を実施し、この研究結果を踏まえて、ネットワーク事業者に関する以下のドキュメント素案を作成した。

- 接続規定　（ネットワーク事業者が全国保健医療情報ネットワークに接続する際に求められるネットワーク接続方式）
- 接続認定要件　（全国保健医療情報ネットワークに接続する際に遵守すべきセキュリティ基準）
- 運用ガイドライン　（全国保健医療情報ネットワークに接続するネットワーク事業者向けの障害時対応、監視方法、利用申請方法等のガイドライン）

5.4. 各組織と素案ドキュメントの関連

本事業で検討した組織と作成した 9 種の素案ドキュメントとの関連を図表 5-1 に示す。

図表 5-1　各組織と素案ドキュメントの関連



6. コスト試算

6.1. 試算の前提条件

6.1.1. コスト試算の目的・方法

接続機関の負担額の妥当性を検証することを目的として、認証主体（登録局・発行局）の設立に係る初期費用（システム開発費用、ネットワーク整備費用、居室整備費用等)、運用費用（設備維持費用、人件費等）を試算し、証明書発行１枚あたりの費用を試算した（試算方法は以下の①②の通り)。

【コスト試算の方法】
①発行局・登録局等の初期費用・ランニング費用（認証に係るコスト）を積算
②認証に係るコストを証明書の想定発行枚数で割り戻すことにより、
１枚あたりの証明書発行コストを試算

6.1.2. コスト試算の条件

コスト試算における変動要素として、「認証局全体のシステム構成」「証明書の発行枚数」の２点が挙げられる。「認証局全体のシステム構成」によって、システム開発等の初期費用・維持費用が変動し、証明書の発行枚数によって人員体制等が変動するため、これらの２点についてそれぞれパターンを設定し、各パターンにおけるコスト試算を実施した。

（１）認証局全体のシステム構成のパターン設定と試算範囲

認証局全体システム構成を

図表 6-1 の A～C の 3 構成で仮にパターン設定し、それぞれのコストを検討した。

なお、構成 C（松）については、参考として、仮にオンライン証明書申請等により、「データ入力作業の削減」「印刷作業/発送作業の削減」を実現できた場合のコスト試算を示している（また、オンライン申請の実運用では、医療機関からの直接のオンライン申請ではなく、ネットワーク事業者等の代行者による申請が想定される）。

本コスト試算における試算範囲は

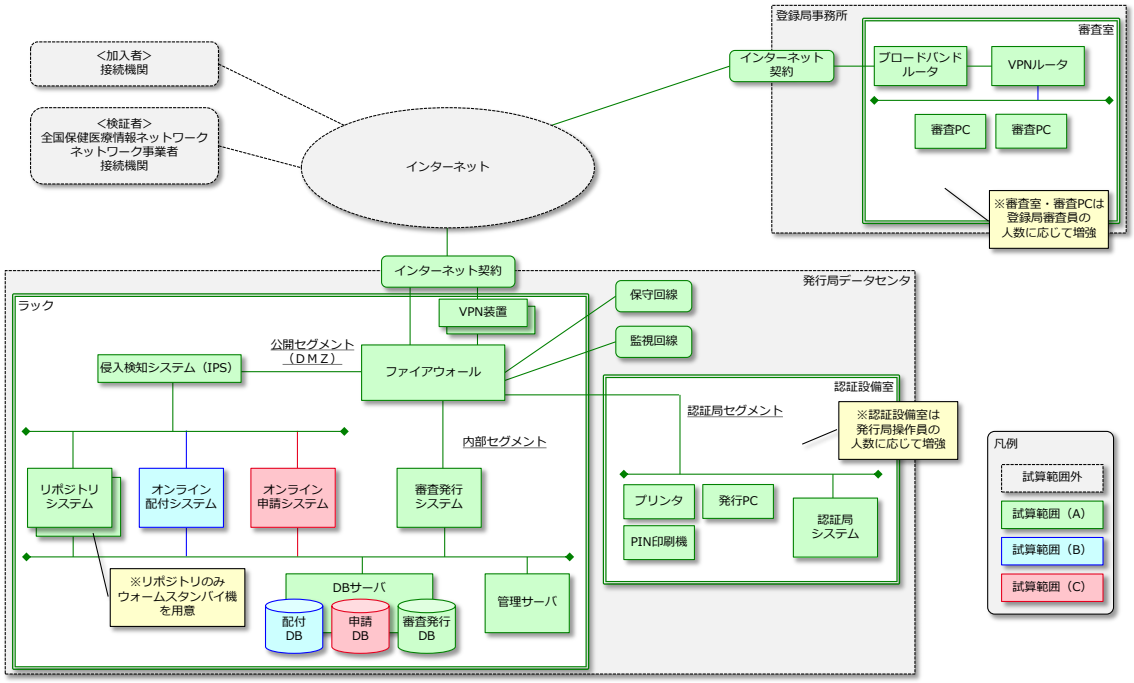
図表 6-2 の通りである。

図表 6-1　認証局のシステム構成の設定[19]

構成／認証局機能	申請（接続機関 →登録局）	配付（発行局 →接続機関）
A（梅）シングル構成 オフライン証明書申請 オフライン証明書配付	郵送申請 ・申請書(原紙) ・指定通知書(コピー) ・チェックシート(原紙)	・証明書媒体郵送(書留) ・PIN 封筒郵送(書留) ★証明書 PIN 記載
導入効果・目的	―	
B（竹）冗長構成 オフライン証明書申請 オンライン証明書配付	郵送申請 ・申請書(原紙) ・指定通知書(コピー) ・チェックシート(原紙)	・証明書媒体(郵送なし) ★ダウンロードする ・PIN 封筒郵送(書留) ★証明書 PIN 記載 ★ダウンロード ID 記載 ★ダウンロードキー記載
導入効果・目的	・発行局業務省力化（媒体梱包/媒体発送作業を削減） ・費用削減（媒体費/媒体郵送費を削減）	
＜参考＞ **C（松）冗長構成** オンライン証明書申請 オンライン証明書配付	オンライン申請 ・申請書(WEB) ★メール登録(連絡用) ★ダウンロード ID 生成 ★ダウンロードキー生成 ★証明書 PIN 生成 ・指定通知書(画像データ) ・チェックシート(WEB) ・電子署名／検証	・証明書媒体(郵送なし) ★ダウンロードする ・PIN 封筒(郵送なし) ★申請時に生成 ・メール通知 ★審査発行完了を通知
導入効果・目的	・登録局業務省力化（データ入力作業を削減） ・発行局業務省力化（媒体梱包/媒体発送作業を削減） ・費用削減（媒体費/媒体郵送費を削減） ・発行局業務省力化（PIN 印刷/PIN 発送作業を削減） ・費用削減（PIN 郵送費を削減）	

[19] 下線は構成 B（竹）の場合に構成 A（梅）に追加される機能・業務・効果を指す。二重下線は構成 C（松）の場合に追加される機能・業務・効果を指す。表中の用語は、下記の通り。「チェックシート」：セキュリティ基準の準拠性を立証するためのものである。「証明書 PIN」：電子証明書(PKCS#12 形式)を活性化するためのものである。「ダウンロード ID」：電子証明書をダウンロードする際の ID を指す。「ダウンロードキー」：電子証明書をダウンロードする際のパスワード（ID とセット）を指す。

図表 6-2　コスト試算範囲



（２）証明書の発行枚数

証明書の発行枚数により、必要な人員体制等が変動するため、証明書の発行枚数を1ヶ月あたり 250 枚・750 枚・1,500 枚・3,000 枚・4,500 枚とパターン設定し、各パターンにおけるコストを試算した。

なお、本試算においては、1 月あたり 750 枚～1,500 枚程度を初期の基準枚数として見込んでいる。

6.2. 初期費用の設定

認証主体の整備に関する初期費用として、登録局・発行局・その他に関する費用項目を設定し、各パターンに応じたコストを試算した。各項目の内容は**エラー! 参照元が見つかりません。**の通りである。

図表 6-3　システム構成パターン別の認証局機能と設備

項目／構成概要			構成 A（梅） シングル構成	構成 B（竹） 冗長構成	構成 C（松） 冗長構成
認証局機能	オフライン証明書申請		対応	対応	－
	オフライン証明書配付		対応	－	－
	オンライン証明書申請		－	－	対応
	オンライン証明書配付		－	対応	対応
設備	発行局	認証設備室	○	○	○
		ネットワークインフラ	△	◎	◎
		認証局システム	△	◎	◎
		リポジトリシステム	△	◎	◎
		審査・発行システム	△	◎	◎
		オンライン証明書配付システム	－	◎	◎
		オンライン証明書申請システム	－	－	◎
	登録局	審査室	○	○	○
		ネットワークインフラ	○	○	○
		審査 PC	○	○	○

○：整備、◎：冗長構成で整備、△：シングル構成で整備

図表 6-4　システム構成パターン別の初期費用

発行枚数（枚）のパターン						
1ヶ月間の発行枚数		250	750	1,500	3,000	4,500
1年間の発行枚数		3,000	9,000	18,000	36,000	54,000
6年間の発行枚数		18,000	54,000	108,000	216,000	324,000
初期費用（千円）						
構成A（梅）	初期費用	123,100	123,900	125,700	129,300	132,900
	うち発行局	105,400	105,400	105,400	105,400	105,400
	うち登録局	1,200	2,000	3,800	7,400	11,000
	うち共通費	16,500	16,500	16,500	16,500	16,500
構成B（竹）	初期費用	199,900	200,700	202,500	206,100	209,700
	うち発行局	182,200	182,200	182,200	182,200	182,200
	うち登録局	1,200	2,000	3,800	7,400	11,000
	うち共通費	16,500	16,500	16,500	16,500	16,500
構成C（松）	初期費用	247,000	247,000	247,400	248,800	249,600
	うち発行局	229,300	229,300	229,300	229,300	229,300
	うち登録局	1,200	1,200	1,600	3,000	3,800
	うち共通費	16,500	16,500	16,500	16,500	16,500

6.3. 運用費用

認証主体における運用費用として、設備維持費（登録局関連・発行局関連）、人件費について試算した。

（１）設備維持費（発行局・登録局）

設備維持費として、月額 300 万円～600 万円程度の費用を見込む。

図表 6-5　システム構成パターン別の設備維持費

発行枚数（枚）のパターン						
1 ヶ月間の発行枚数		250	750	1,500	3,000	4,500
1 年間の発行枚数		3,000	9,000	18,000	36,000	54,000
6 年間の発行枚数		18,000	54,000	108,000	216,000	324,000
月額設備維持費（千円）						
構成 A（梅）	月額設備維持費	3,700	3,700	3,900	4,300	4,700
	うち発行局	3,400	3,400	3,400	3,400	3,400
	うち登録局	300	300	500	900	1,300
構成 B（竹）	月額設備維持費	5,700	5,700	5,900	6,300	6,700
	うち発行局	5,400	5,400	5,400	5,400	5,400
	うち登録局	300	300	500	900	1,300
構成 C（松）	月額設備維持費	6,000	6,000	6,000	6,200	6,200
	うち発行局	5,700	5,700	5,700	5,700	5,700
	うち登録局	300	300	300	500	500

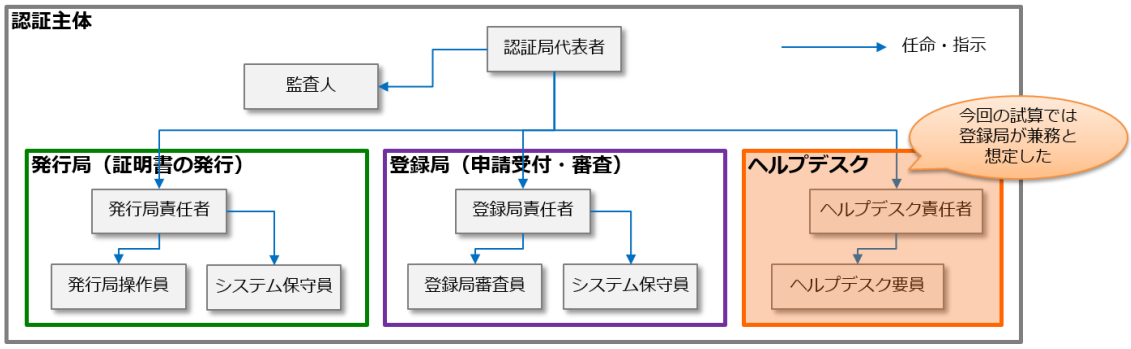
（２）人件費

認証局の運営に最低限必要と想定される体制は図表 6-6、図表 6-7 の通り、認証局代表者・監査人等の認証主体の設立・運営に必要な人員、及び登録局・発行局の運営に係る人員が必要となる。

ただし、人員体制は証明書発行枚数によって大きく変動するため、証明書発行枚数の想定枚数ごとに、システム構成パターン別に必要な人員体制・人件費を試算した。（

図表 6-8）なお、人件費の試算にあたっての人件費は法定福利費も含めた費用として試算している。発行枚数・システム構成にもよるが、10 人～20 人程度の人員体制が必要となり、人件費は月額 500 万円～2,000 万円弱程度の費用が発生する。

図表 6-6　認証主体の体制図（本コスト試算での想定案）



図表 6-7　認証主体の人員体制の試算方法

所属	担当名	最低配置人数（案）	主な役割	試算方法
認証主体	認証局代表者	1 名	運営主体の運営及び管理と業務の統括	運営主体の役員等との兼務が考えられ稼働率を 50%に設定。
	監査人	2 名	内部監査の実施	毎年 12 日のみの稼動と想定し稼働率を 5%に設定。
登録局	登録局責任者	1 名	登録局の運営及び管理と業務の統括	発行局は外注可能と想定。他サービスと兼務可能なため、発行枚数に応じて稼働率を設定。
	登録局審査員	2 名	接続機関からの申請受付・審査	
	システム保守員	1 名	登録局のシステム保守	月あたりの稼働率を 10%に設定。
発行局	発行局責任者	1 名	発行局の運営及び管理と業務の統括	専業となることが想定されるため、稼働率を 100%に設定。
	発行局操作員	2 名	機関認証用証明書の発行・失効	
	システム保守員	1 名	発行局のシステム保守	発行局システム保守員が兼務することとし要員を 0 名に設定。
ヘルプデスク※必要に応じて設置	ヘルプデスク責任者	0 名	ヘルプデスクの運営及び管理と業務の統括	主に申請や審査に関する問合せが想定されるため、登録局責任者及び登録局審査員が兼務することとし要員を 0 名に設定。
	ヘルプデスク要員	0 名	接続機関からの問合せ等の対応	

図表 6-8　システム構成パターン別の人件費

発行枚数（枚）のパターン						
1ヶ月間の発行枚数		250	750	1,500	3,000	4,500
1年間の発行枚数		3,000	9,000	18,000	36,000	54,000
6年間の発行枚数		18,000	54,000	108,000	216,000	324,000
人員体制（人）・月額人件費（千円）						
構成A（梅）	人員体制	10	14	20	34	48
	月額人件費	5,500	10,620	18,300	32,300	46,300
構成B（竹）	人員体制	10	14	20	32	44
	月額人件費	4,940	9,220	15,500	28,200	40,900
構成C（松）	人員体制	10	10	12	16	20
	月額人件費	4,940	5,080	7,220	11,500	15,920

6.4. 認証主体のコスト試算及び証明書発行１枚あたりの費用の試算

（１）認証主体の初期費用・運用費用の試算結果

「6.1 試算の前提条件」の前提条件に基づいて、「6.2 初期費用の設定」及び「6.3 運用費用」の試算結果をまとめると総費用は図表 6-9 の通りとなる（設備維持費・人件費は 6 年間の総費用として設定）。

図表 6-9　初期費用・運用費用の試算結果

発行枚数（枚）のパターン						
1 ヶ月間の発行枚数		250	750	1,500	3,000	4,500
1 年間の発行枚数		3,000	9,000	18,000	36,000	54,000
6 年間の発行枚数		18,000	54,000	108,000	216,000	324,000
総費用（千円）						
構成 A（梅） 6 年間の総費用		839,500	1,316,940	2,048,100	3,412,500	4,776,900
	うち初期費用	123,100	123,900	125,700	129,300	132,900
	うち設備維持費	266,400	266,400	280,800	309,600	338,400
	うち人件費	396,000	764,640	1,317,600	2,325,600	3,333,600
	うち証明書実費	54,000	162,000	324,000	648,000	972,000
構成 B（竹） 6 年間の総費用		991,180	1,350,540	1,894,500	2,992,500	4,090,500
	うち初期費用	199,900	200,700	202,500	206,100	209,700
	うち設備維持費	410,400	410,400	424,800	453,600	482,400
	うち人件費	355,680	663,840	1,116,000	2,030,400	2,944,800
	うち証明書実費	25,200	75,600	151,200	302,400	453,600
構成 C（松） 6 年間の総費用		1,050,880	1,093,360	1,296,440	1,717,600	2,133,840
	うち初期費用	247,000	247,000	247,400	248,800	249,600
	うち設備維持費	432,000	432,000	432,000	446,400	446,400
	うち人件費	355,680	365,760	519,840	828,000	1,146,240
	うち証明書実費	16,200	48,600	97,200	194,400	291,600

（２）証明書発行１枚あたりの年間費用の試算

コスト試算結果を踏まえて、証明書発行 1 枚あたりの年間費用を試算した。なお、証明書発行 1 枚あたりの費用としては、初期費用で整備するシステム・ネットワーク等は 6 年で更新する前提とし、運営 6 年間分の運用費用と初期費用を賄うために必要な費用を試算することとした。

証明書発行１枚あたりの年間費用＝ （初期費用＋ランニング費用 72 か月分）／72 ヶ月の合計発行枚数／6 年間

上記の方法にて試算した結果を図表 6-10 に示す。効率的な審査・発行が可能な構成 B・C の場合、発行枚数が多いほど 1 枚あたりの費用が安くなる（参考で試算した構成 C は更にその傾向が顕著)。証明書 1 枚あたりの年間費用は、いずれの構成においても 2,000 円～4,000 円程度となり、

図表 6-11 における他のパブリック認証局の証明書費用を鑑みても、本コスト試算結果は接続機関側に過度な負担を強いるものではないといえる。

また、実運用では医療機関等からの申請の際に、１回の審査で複数枚の証明書を発行することが想定される。この場合においては、追加の審査費用は発生しないため、証明書１枚あたりの費用は低減でき、より安価に提供することが可能となる。

図表 6-10　証明書１枚あたりの年間費用

発行枚数（枚）のパターン					
１ヶ月間の発行枚数	250	750	1,500	3,000	4,500
１年間の発行枚数	3,000	9,000	18,000	36,000	54,000
６年間の発行枚数	18,000	54,000	108,000	216,000	324,000
パターン別の証明書１枚あたりの年間費用（円）					
構成 A（梅）	7,773	4,065	3,161	2,633	2,457
構成 B（竹）	9,178	4,168	2,924	2,309	2,104
構成 C（松）	9,730	3,375	2,001	1,325	1,098

図表 6-11　証明書費用の参考データ

#	認証局名／証明書名	説明	用途	年間費用（円）
1	オンライン請求システム専用認証局	審査支払機関が自身の業務のために用意したプライベート認証局。 ■4,000 円／38 ヶ月	クライアント認証	1,263
2	商業登記電子証明書	商業登記に基づく電子認証制度。 実印レベルの効力。 ■16,900 円／27 ヶ月	電子署名	7,511
3	J 社電子証明書サービス	電子署名及び認証業務に関する法律による認定認証業務（特定認定認証サービス）。 実印レベルの効力。 ■33,000 円／58 ヶ月	電子署名	6,828
4	某社クライアント証明書サービス	ブラウザにルート証明書が登録されているパブリック認証局が発行するクライアント証明書。 審査業務は別途必要。 ■8,400 円／12 ヶ月	クライアント認証 電子署名	8,400
5	某社サーバ証明書サービス	ブラウザにルート証明書が登録されているパブリック認証局が発行するサーバ証明書。 ■55,000～220,000 円／12 ヶ月	サーバ認証	55,000 ～ 220,000

7. 接続検証

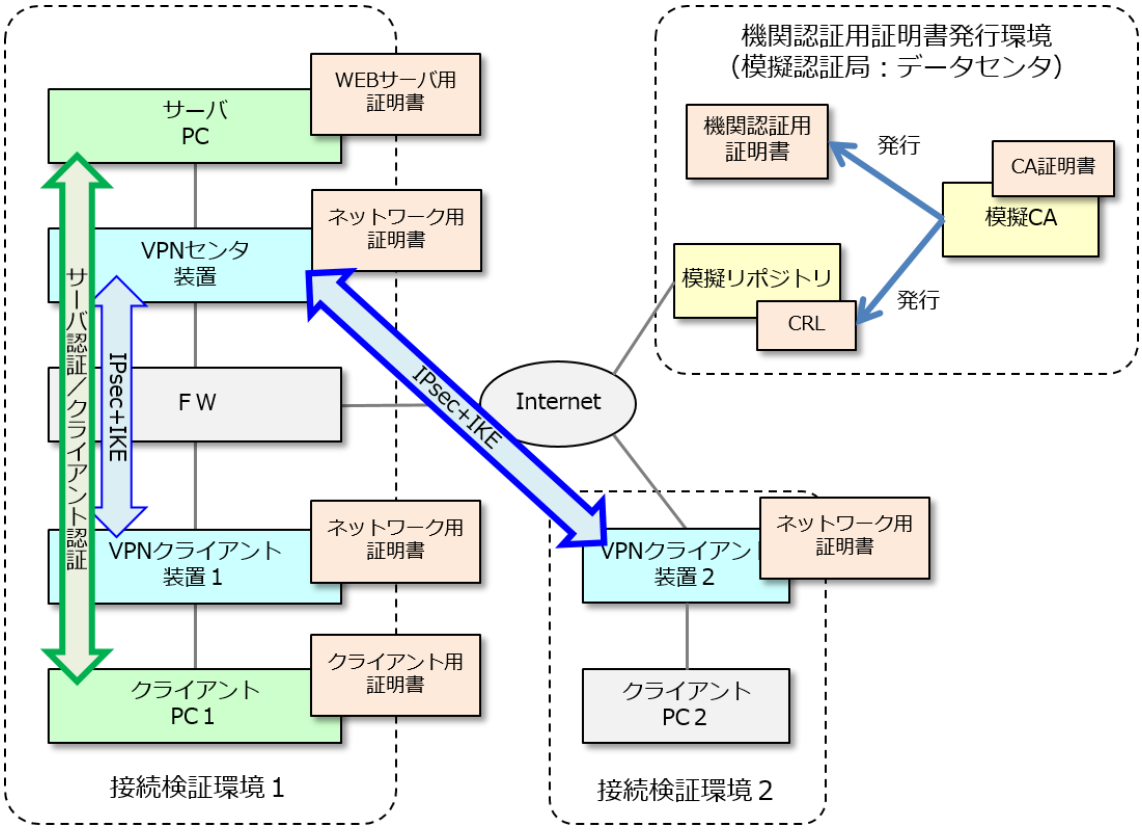
7.1. 検証目的と対象

認証局運用規程（CPS）に定義した証明書プロファイルの正しさを検証するため、IPsec+IKE 方式による VPN 接続検証と TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続検証を実施した。検証のために模擬認証局を構築し機関認証用証明書を発行した。

7.2. 検証環境の構築

検証環境として図表 7-1 に示す機関認証用証明書発行環境、接続検証環境を構築した。

図表 7-1 検証環境



7.3. 検証機材及び機関認証用証明書の内容

検証環境の構築に際して準備した機材等を図表 7-2 に示す。

図表 7-2 検証機材等

No	名称	説明・型番等
1)	CA 証明書	模擬 CA より発行
2)	ネットワーク用証明書	模擬 CA より PKCS#12 形式にて発行
3)	WEB サーバ用証明書	模擬 CA より PKCS#7 形式にて発行
4)	クライアント用証明書	模擬 CA より PKCS#12 形式にて発行
5)	CRL	模擬 CA より発行
6)	VPN センタ装置	Cisco ASA5585-X
7)	VPN クライアント装置 1、2	三菱電機 smartstar
8)	サーバ PC	Windows 8.1
9)	クライアント PC1	Windows 10
10)	クライアント PC2	Windows 7

模擬認証局より発行した機関認証用証明書内容を図表 7-3 に示す。

図表 7-3 機関認証用証明書内容

種類	証明書項目	証明書記載内容
CA 証明書	Issuer / Subject	CN = HPKI-01-TEST_ROOT_CA-forAuthentication-forOrganization OU = TEST ROOT CA Center O = Japannet Corporation C = JP
	KeyUsage	KeyCertSign, CRLSign
	ExtendedKey Usage	設定なし
	SubjectDirectoryAttributes	設定なし
ネットワーク用証明書（VPN センタ装置）	Subject	SERIALNUMBER = 2010401059681 CN = TRC-ASA-VPN-1 OU = 1.2.392.100495.1.100.1.6.2010401059681.1 OU = medical information service provider O = MIND L = Tokyo C = JP

種類	証明書項目	証明書記載内容
	KeyUsage	DigitalSignature
	ExtendedKeyUsage	設定なし
	SubjectDirectoryAttributes	medical information service provider
ネットワーク用証明書（VPN クライアント装置）	Subject	SERIALNUMBER = 1234567 CN = Japannet Hospital OU = 1.2.392.100495.1.100.1.1.1234567 OU = insurance medical care facility O = JapannetGroup L = Tokyo C = JP
	KeyUsage	DigitalSignature
	ExtendedKeyUsage	設定なし
	SubjectDirectoryAttributes	insurance medical care facility
WEB サーバ用証明書	Subject	SERIALNUMBER = 7010001003845 CN = hasegawakikin OU = 1.2.392.100495.1.100.1.6.7010001003845.1 OU = medical information service provider O = JN L = minatoku C = JP
	KeyUsage	DigitalSignature, KeyEncipherment
	ExtendedKeyUsage	serverAuth, clientAuth
	SubjectDirectoryAttributes	medical information service provider
クライアント用証明書	Subject	SERIALNUMBER = 1234567 CN = Japannet Hospital OU = 1.2.392.100495.1.100.1.1.1234567 OU = insurance medical care facility O = JapannetGroup L = Tokyo C = JP
	KeyUsage	DigitalSignature

種類	証明書項目	証明書記載内容
	ExtendedKeyUsage	clientAuth
	SubjectDirectoryAttributes	insurance medical care facility

7.4. 検証内容

検証環境にて検証した内容について以下に記載する。

（１）機関認証用証明書のインストール検証

模擬 CA から発行したネットワーク用証明書及び CA 証明書を VPN センタ装置と VPN クライアント装置 1、2 へインストールした。同様に模擬 CA から発行した WEB サーバ用証明書及び CA 証明書をサーバ PC へ、クライアント用証明書及び CA 証明書をクライアント PC1 へインストールした。

（２）IPsec+IKE 方式による VPN 接続検証

VPN センタ装置と VPN クライアント装置間で IPsec+IKE 方式による VPN 接続検証を実施した。検証に際して設定した IKEv2 及び IPsec のパラメータを図表 7-4 に示す。

図表 7-4 IKEv2 及び IPsec のパラメータ

区分	項目	内容
IKEv2 パラメータ	相互認証方式	RSA 電子署名認証方式
	暗号化アルゴリズム	AES-128 CBC モード
	疑似乱数関数	AES-XCBC-PRF-128
	Diffie-Hellman グループ	2048 ビット MODP グループ（グループ 14）
IPsec パラメータ[20]	暗号化アルゴリズム	AES-128 CBC モード
	認証アルゴリズム	AES-XCBC-MAC-96

（３）TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続検証

VPN センタ装置の後方に設置するサーバ PC 上で動作する WEB サーバと、VPN クライアント装置 1 の後方に設置するクライアント PC1 上で動作する WEB ブラウザ間で、TLS1.2 によるサーバ認証／クライアント認証の HTTPS 接続検証を実施した。検証に際して使用した WEB サーバ及び WEB ブラウザの設定を図表 7-5 に示す。

[20]出典：IPsec パラメータは「オンデマンド VPN（HEASNET 版）相互接続仕様書 v1.2」に基づく。

図表 7-5 WEB サーバ及び WEB ブラウザの設定

区分	項目	内容
WEB サーバ（サーバ PC）	WEB サーバソフトウェア	Apache 2.4.29
	暗号化ソフト	OpenSSL 1.1.0g
	プロトコルバージョン	TLS1.2
	暗号スイートの設定	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256
WEB ブラウザ（クライアント PC）	WEB ブラウザソフト	Internet Explorer 11
	WEB ブラウザの設定	デフォルト設定

7.5. 検証結果

検証環境にて検証した結果について以下に記載する。

（１）機関認証用証明書のインストール検証結果

検証結果を図表 7-6 に示す。

図表 7-6 機関認証用証明書のインストール検証結果

No	検証項目	検証結果
1-1	VPN センタ装置にネットワーク用証明書及び CA 証明書をインストールできるか	○
1-2	VPN クライアント装置 1、2 にネットワーク用証明書及び CA 証明書をインストールできるか	○
1-3	サーバ PC に WEB サーバ用証明書及び CA 証明書をインストールできるか	○
1-4	クライアント PC1 にクライアント用証明書及び CA 証明書をインストールできるか	○

○：できた、×：できなかった

（２）IPsec+IKE 方式による VPN 接続検証結果

検証結果を図表 7-7 に示す。

図表 7-7 IPsec+IKE 方式による VPN 接続検証結果

No	検証項目	検証結果
2-1	VPN 接続ができるか	○
2-2	トラストアンカ及び証明書パスの検証ができるか	○
2-3	有効期間の確認ができるか	○
2-4	CRL を用いて失効確認ができるか	○
2-5	Subject-OrganizationUnitName に記載の機関用 OID を用いて制御ができるか	○
2-6	SubjectDirectoryAttributes に記載の hcRole を用いて制御ができるか	×
2-7	Subject-OrganizationUnitName に記載の hcRole を用いて制御ができるか	○
2-8	ログに機関用 OID を記録できるか	○

○：できた、×：できなかった

（３）TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続検証結果

検証結果を図表 7-8 に示す。

図表 7-8 TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続検証結果

No	検証項目	検証結果
3-1	TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続ができるか	○
3-2	トラストアンカ及び証明書パスの検証ができるか	○
3-3	有効期間の確認ができるか	○
3-4	CRL を用いて失効確認ができるか	○
3-5	Subject-OrganizationUnitName に記載の機関用 OID を用いて制御ができるか	×
3-6	SubjectDirectoryAttributes に記載の hcRole を用いて制御ができるか	（－）
3-7	Subject-OrganizationUnitName に記載の hcRole を用いて制御ができるか	○
3-8	ログに機関用 OID を記録できるか	（－）

○：できた、×：できなかった、（－）：未実施

7.6. 考察

以上の検証結果より、ネットワークレベル及びアプリケーションレベルでの PKI 認証おいて、本事業で検討した機関認証用証明書を、技術的に利用できることが確認できた。検証結果のうち「×：できなかった」、「(－)：未実施」の検証項目について以下に考察する。

（１）IPsec+IKE 方式による VPN 接続検証結果の考察

図表 7-7 の No.2-6 の結果について、現時点で SubjectDirectoryAttributes に設定した hcRole を適切に処理できる機器が存在しないと考えられるため、結果は妥当なものと考えられ、今後、適切に処理できる機器の登場を期待したい。なお、hcRole での制御のみを目的とすれば No.2-7 の結果より、Subject-OrganizationUnitName に設定した hcRole にて代替可能であるといえる。

（２）TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続検証結果の考察

図表 7-8 の No.3-5、3-6、3-8 の結果について、本事業では WEB サーバソフトウェアの基本機能のみで検証しており、WEB サーバ上で細かな PKI 認証処理を実装できなかったため、結果は妥当なものであると考えられる。実際の利用シーンにおいては、サービス事業者は WEB サーバのみでなく WEB サーバアプリケーションを構築することが想定されるため、PKI 認証処理を適切に実装すれば制御可能な項目であると考えられる。

8. まとめ

本事業では、全国保健医療情報ネットワークに接続する機関認証主体についてや機関認証方式、ネットワーク事業者の接続規定の調査・研究を実施し、実施内容を基に証明書ポリシや認証局の要件、認証局の運用規程、接続のセキュリティポリシーの必要な技術文書について、素案を策定した。策定した結果、機関認証主体の開設に必要となる文書を整備することができた。ただし機関認証主体の運用業務については、相互認証基盤との役割の整理や、接続機関に対する審査の効率化や正確性を向上するための、より具体的な検討が必要と考える。以下に、今後の課題と提言を示す。

8.1. 今後の課題

（１）相互認証基盤の事業主体との役割の整理

本事業では、機関認証主体の役割として、審査業務において機関認証用証明書を発行する接続機関の実在性や申請意思、有資格性に加え、セキュリティ要件を満たすことの確認を実施すると整理した。このため、機関認証主体があることにより、相互接続基盤の事業主体の負担軽減につながると考える。

一方、相互接続基盤に関する実証を行った総務省実証事業においても接続機関の接続規定やセキュリティ規定を作成しており、相互接続基盤の事業主体が接続機関のセキュリティ要件を審査することを想定していると考えられ、審査内容が重複する。

そのため、今後機関認証主体並びに相互接続基盤の事業主体が具体化した際には、双方の間で役割分担を確認し、確認した役割における機関認証主体に対する要件を再整理する必要があると考える。

（２）機関認証のユースケースの整理と認証対象機関の拡大

本事業において、接続機関として以下 5 種類を想定し、業種に合わせた機関認証主体による審査方法を定義した。

1) 保険医療機関
2) 保険薬局
3) 地域医療情報連携ネットワークの事業主体
4) 介護保険法における介護事業者
5) 医療情報共有サービスを提供する民間事業者

しかし全国保健医療情報ネットワークに接続する機関は、本事業で認証対象とした 5 業種に限らないと考えられ、接続機関として新たな業種が加わった場合には、改めてその機関の審査方法を定義しなければならない。

機関認証が必要となる接続機関の考え方として、本事業では検討対象外とした、機関認証を必要とするユースケースを整理することで、接続機関を明らかにできると考えられる。今後相互接続基盤に関する検討がさらに具体化するとともに、ユースケースの検討も多様化することが期待される。

（３）介護事業者における指定通知書の確認方法

本事業における介護事業者の認定基準は、本報告書「2.4.3 認定基準について（2）介護事業者、保険医療機関、保険薬局の認定基準」に記載した通り、「指定通知書」を有しており、「指定通知書」が有効であることとした。

このため、認証主体は、介護事業者から提出される「指定通知書コピー」に記載されている情報を基に、都道府県・市町村の公開情報を確認もしくは介護サービス公表システム等を確認して、当該介護事業者の実在性と有資格性を確認しなければならない。

しかしながら、指定を受けた介護事業者の情報については、公示の義務はあるが、情報公開方法については都道府県・市町村に任されており、統一されていないことが調査により判明した。

そのため、各都道府県・市町村における介護事業者の情報公開状況の調査が必要である。また、将来的に各地方厚生局が保険医療機関・保険薬局の情報を統一的に公開しているように、介護事業者の公開方法についても、都道府県・市町村で統一化が図られるべきと考える。統一化することにより、機関認証主体が介護事業者の審査で利用するだけでなく、今後日本において介護事業者の役割がますます高くなるなか、国民が介護事業者の情報を知るための統一的な基盤が実現できるのではないかと考える。

（４）ネットワーク接続サービスの適合性評価基準と第三者評価機関

本事業では、全国保健医療情報ネットワークへ接続するためのネットワーク事業者が提供するネットワーク接続サービスは、第三者評価機関による「医療情報システムの安全管理に関するガイドライン」への適合性評価を受けることを要件とした。このため、ネットワーク事業者が提供するネットワーク接続サービスを対象として、ガイドラインへの適合性評価基準と、その適合性評価を実施する第三者評価機関が必要である。

しかし現在、レセプトオンライン請求を目的とした HISPRO による「支払基金等へのレセプトオンライン請求用 IPsec＋IKE サービス」の適合性評価基準は存在するが、全国保健医療情報ネットワークへの接続を目的としたネットワーク接続サービスの適合性評価基準は存在しない。

そのため、全国保健医療情報ネットワークへの接続を目的とした、ネットワーク接続サービス（IP-VPN、IPsec+IKE、専用線等）の適合性評価基準を策定し、その適合性評価基準に沿って適合性評価を実施する第三者評価機関の整備が必要と考える。

以上のように、第三者評価機関を整備することで、接続機関に対して全国保健医療情報ネットワークへの安全かつ信頼性の高いネットワーク接続サービスが提供できるものと考える。

（５）接続機関（レスポンダ）の適合性評価基準と第三者評価機関

本事業では、全国保健医療情報ネットワークへレスポンダとして接続する接続機関（主にサービス事業者）に対する機関認証主体によるセキュリティ基準の審査方法として、第三者評価機関による三省 4 ガイドラインへの適合性評価を受けることを要件とした。このため、サービス事業者が提供する医療情報共有サービスを対象として、ガイドラインへの適合性評価基準と、適合性評価を実施する第三者評価機関が必要である。

ASP・SaaS サービスを提供するサービス事業者を対象とした場合は、HISPRO による「民間事業者による医療情報の外部保存及びＡＳＰ・ＳａａＳサービス」の適合性評価基準が存在するため、この適合性評価基準を全国保健医療情報ネットワーク上の ASP・SaaS サービスでも活用することが考えられ、適用可能なものかの検討が必要である。

また、クラウドサービスを提供するサービス事業者を対象とした場合は、現在、クラウドサービスのセキュリティ対策ガイドラインは存在するが、サービス事業者向けのガイドラインは存在せず、適合性評価基準とその第三者評価機関も存在しない。

そのため、今後策定されるであろうクラウドサービス事業者向けガイドラインを基準として、適合性を適切に評価する適合性評価基準を策定し、その適合性評価基準に沿って適合性評価を実施する第三者評価機関の整備が必要と考える。

以上のように、第三者評価機関を整備することにより、機関認証主体によるセキュリティ基準の審査が実施できるとともに、接続機関に対して全国保健医療情報ネットワークを介した安全かつ信頼性の高い医療情報共有サービスが提供できるものと考える。

（６）接続機関（レスポンダ）のセキュリティ基準の審査方法

本事業では、全国保健医療情報ネットワークへレスポンダとして接続する接続機関に対する機関認証主体によるセキュリティ基準の審査方法として、一律に第三者評価機関による三省 4 ガイドラインへの適合性評価を受けることを要件とした。しかしながら、第三者評価に対応するための接続機関の費用や手間を考慮すると、特に地連事業主体や地域の中核病院等において参入の妨げになることが想定される。

このため、機関認証主体によるセキュリティ基準の審査方法として、本事業で検討した「第三者評価」よりは安価で手間がかからず、「自己申告」よりは信頼性が高い審査方法を検討する必要がある。例えば、地連事業主体や地域の中核病院等の場合には、ホームページ等で「準拠性チェックシート」の自己チェック結果を他の接続機関に公開することを前提に、機関認証主体では「自己申告」にて審査を行う等の方法が想定される。ただし現時点では議論が不十分であるため、今後検討していく必要があると考える。

（７）ネットワーク認証方式の違いによるアクセス制御方式

本事業では、ネットワーク事業者が提供するネットワーク接続サービスのネットワーク認証方式について、機関認証主体が発行する機関認証用証明書を利用することは、ネットワーク事業者の判断に委ねることとした。しかしながら、全国保健医療情報ネットワーク内では、サービス事業者のセキュリティポリシーにより、ネットワーク認証方式に機関認証用証明書の利用を必要とするサービスと、必要としないサービスが混在することが想定される。

このため、混在するサービス事業者のセキュリティポリシーを満たすようなアクセス制御方式の検討が必要である。例えば、ネットワーク事業者のゲートウェイにて、ネットワーク認証方式が、機関認証用証明書を利用したものか、利用していないものかを判定し、適切にアクセス制御する方式等が考えられる。

以上のような案が考えられるが、現時点では議論が不十分であること、相互接続基盤の事業主体、ネットワーク事業者、サービス事業者等の関係者の役割や責任範囲等の整理が必要であることから、今後検討していく必要があると考える。

（８）通信サービス提供者の役割と提供範囲の整理

本事業では、通信サービス提供者のひとつとして、相互接続基盤と接続機関との間のネットワーク接続を提供するネットワーク事業者について検討した。他の通信サービス提供者として、相互接続基盤を提供する通信サービス提供者や、地域医療情報連携ネットワークを提供する通信サービス提供者等が存在すると考えられる。

このため、全国保健医療情報ネットワークの運営、提供においては、本事業で検討したネットワーク事業者、相互接続基盤を提供する通信サービス提供者、地域医療情報連携ネットワークを提供する通信サービス提供者等の役割や提供範囲等を確認し、運営、提供体制について整理する必要があると考える。

（９）接続機関の増加に伴う機関認証主体の対応

本事業では、機関認証主体の業務について、オフラインでの証明書申請及び証明書配付を前提に業務内容の検討を実施した。また、本報告書「6 コスト試算」にて、接続機関増加に伴う審査、発行件数拡大に応じた人員体制の強化が必要であり、特にオフラインでの証明書申請及び証明書配付の場合は機関認証主体の運営コストが増大していく結果を示した。

以上の結果から、機関認証主体の運営を維持するためには運営コスト増大の抑制が必要であり、そのためには接続機関の増加を考慮した業務効率化の検討が必要である。具体的には、オンライン証明書申請やオンライン証明書配付等を実現することにより、審査、発行業務の効率化や、電子証明書を格納する媒体費用や郵送費用の削減等が期待でき、今後検討していく必要があると考える。

（１０）機関用 OID 利用時の留意点

本事業では保険医療機関や保険薬局向けの機関用 OID には医療機関番号を用いるよう整理した。さらに 7 桁の医療機関番号では都道府県の識別ができない、医療機関番号が再利用される可能性があるといった課題を解決し、一意性を持たせた。解決策の 1 つとして、機関用 OID の最下位に指定通知書に記載された「指定の期間」の開始日（8 桁固定の番号）を設定するため、機関認証用証明書に設定される機関用 OID は、指定通知書の有効期間同様、6 年毎に変わる。

このため、認証情報として機関用 OID を利用するサービスでは、機関用 OID の最下位が 6 年以内であるか確認したり、機関用 OID の最下位を認証情報として利用しないといった処理を行うか、もしくは 6 年毎に機関用 OID を登録し直す必要がある。

8.2. 提言

（１）機関認証主体業務の実証

本事業で検討した認証主体による審査を実施することにより、実在性、有資格性、所在地、セキュリティの確認が可能となる機関認証が実現できると考える。保険医療機関・保険薬局・介護事業者・地連事業主体・サービス事業者の審査方法、及び証明書配布フロー等、認証主体の運用に必要となる業務の検討を行い、決めなければならない事項について方向性が定められたと考える。ただし、机上での検討、及びジャパンネットが認証局運用業務の経験から導き出した結論であり、実際に審査業務や証明書の配付を実施していない。

このため、本報告書「6 コスト試算」で前提条件とした、審査業務の時間、証明書発行時間、及び人件費、また本事業で検討した審査方法等の正当性が実運用にて確認が出来ていないため、認証主体の業務を想定した実運用を検証するための実証を行い、本報告書「6 コスト試算」で試算した結果の確認が必要であると考える。

また、併せて本報告書「8.1.（３）介護事業者における指定通知書の確認方法」に記載した、各都道府県・市町村における介護事業者の指定通知書の確認方法の整理や、本報告書「8.1.（９）接続機関の増加に伴う機関認証主体の対応」に記載した、オンラインでの証明書申請及び証明書配付による業務効率化の効果測定も実施することが必要であると考える。

なお、実際に保険医療機関・保険薬局の審査を実施して証明書を発行している機関として、社会保険診療報酬支払基金（以下、支払基金）が存在する。本事業では、認証主体自身で接続機関の審査を実施することを想定した審査方法を検討したが、認証主体の審査業務の内、保険医療機関と保険薬局の確認を、例えば支払基金が保持しているデータベースを利用する、もしくは支払基金に審査業務の一部を委託する等の、既存の資源を活用した審査方法の検討も考えられる。

（２）認証対象機関別審査方法の調査

全国保健医療情報ネットワークに接続する機関として、本事業で認証対象とした 5 つの接続機関以外に、対象外とした非保険の医療機関や薬局が考えられる。また総務省実証事業の中間報告において、ユースケースのなかでステークホルダーとして挙げられている行政機関や情報収集機関が認証対象として考えられる。機関毎の実在性や有資格性の審査方法を調査し、認証対象の拡大を実現すべきと考える。

認証対象の拡大を実現することは、医療サービスの多様化に繋がると考えられる。全国保健医療情報ネットワークに直接接続しない患者に対しても利便性向上等の効果が期待できる。

（３）審査業務のシステム化推進

本事業では証明書ポリシから事務取扱要領まで作成し、審査業務の具体化を行っ

た。しかし実際の審査業務を想定した場合、効率性だけでなく正確性の面からも業務のシステム化は必須と考える。

医療機関番号であれば厚生労働省の地方厚生局毎に公開している「コード内容別医療機関一覧表」、法人番号であれば国税庁が公開している「基本３情報」を用いて、医療機関番号または法人番号、機関名、所在地、「コード内容別医療機関一覧表」ではさらに開設者氏名、指定年月日、指定開始を含むデータベースを作成できる。このデータベースを検索するシステムを作成することにより、手入力による入力間違いをなくし、正確な電子データの利用が実現できる。

（４）国際標準への準拠

今後、海外から日本の医療機関を受診する医療ツーリズムにおいて海外から情報の提供を受けることや、海外での手術等に対応した日本からの情報提供の必要性が高まることも考えられることから、認証フレームワークにおいても ISO17090 のような国際標準に準拠していることが望ましい。

また、WTO による国際調達の必要性に鑑みても、調達における公平性、平等性を論理的に説明できるように国際標準への準拠が重要となると考えられる。

参考文献一覧

#	タイトル
(1)	オンライン請求システム専用認証局　運用規程
(2)	保健医療福祉分野 PKI 認証局認証用（組織）証明書ポリシ 1.1 版
(3)	厚生労働省　平成 28 年度　医療情報連携ネットワークにおける標準規格準拠性の検証機関の実現に向けた調査研究業務　別冊報告書『地域間連携を円滑に行うための方策と必要な機能要件にかかる検討』
(4)	保健医療福祉分野ＰＫＩ認証局認証用証明書ポリシ準拠性審査業務実施規則第 1 号様式に基づく監査報告書様式
(5)	医療情報システムの安全管理に関するガイドライン第 5 版
(6)	ASP・SaaS における情報セキュリティ対策ガイドライン
(7)	ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン第 1.1 版
(8)	医療情報を受託管理する情報処理事業者向けガイドライン第 2 版
(9)	クラウドサービス提供における情報セキュリティ対策ガイドライン
(10)	JAHIS HPKI 電子認証ガイドライン V1.1
(11)	経済産業省　平成 22 年度　サービス産業活動環境整備調査事業（医療等情報化共通基盤構築調査事業）『成果報告書』及び『添付資料 SAML 実装仕様書』
(12)	JAHIS『シングルサインオン実装ガイド』及び『JAHIS シングルサインオンにおけるセキュリティガイドライン Ver.1.0』
(13)	チェックリスト項目集（HISPRO 適合性評価）
(14)	厚生労働省 平成 28 年度　医療等分野におけるネットワークの相互接続の実現に向けた調査研究業務　報告書
(15)	厚生労働省　平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業（平成 27 年 3 月）　『運用管理規程』、『緊急時、災害時、障害時の対応手順』
(16)	平成 24 年度以降における厚生労働省統合ネットワーク回線・機器に係る供給（設計・開発、テスト、移行及び運用等）業務一式　調達仕様書
(17)	電気通信分野における情報セキュリティ確保に係る安全基準（第 3 版）
(18)	ネットワークサービスの SLA（サービスレベル合意書）
(19)	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 5 版）（案）
(20)	重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）（案）

参照規格一覧

#	タイトル
(1)	ISO/IS 17090-1:2013 Health informatics - Public key infrastructure Part 1 : Overview of digital certificate services Part 2 : Certificate profile Part 3 : Policy management of certification authority
(2)	X.501 (10/2012) : Information technology - Open Systems Interconnection - The Directory: Models
(3)	X.520 (10/2012) : Information technology - Open Systems Interconnection - The Directory: Selected attribute types

用語集

用語	説明
介護事業者	介護保険法における居宅サービス、地域密着型サービス、居宅介護支援、介護予防サービス等のサービスを提供する事業者。
各種サービスを提供する民間事業者	全国保健医療情報ネットワークを介して、サービスを提供する事業者。
証明書ポリシ	Certificate Policy。電子証明書の利用目的、適用範囲、セキュリティレベル、認証局の責任等、認証局が電子証明書を発行する際の運用方針を示した文書のこと。
全国保健医療情報ネットワーク	厚生労働省において検討している、個人・患者本位で最適な健康管理・診療・ケアを提供するためのネットワーク。「接続機関～ネットワーク事業者」、「ネットワーク事業者～相互接続基盤」、「相互接続基盤～サービス事業者」のネットワーク全体を示す。
相互接続基盤	全国保健医療情報ネットワークの中にある、インターネットエクスチェンジ（Internet Exchange point）。インターネットサービスプロバイダ（Internet Service Provider）の相互接続点として、経済的な接続環境によるインターネット接続コストの低減、接続ホップ数の削減によるバックボーンの品質向上等の役割が期待されており、インターネットのネットワークのなかできわめて重要な位置を占める。
地域医療情報連携ネットワーク	情報通信技術を活用し、複数の医療機関で患者の情報共有を行うために構築されたネットワーク。
データヘルス改革推進本部	平成 29 年 1 月 12 日に厚生労働省で立ち上げた、健康・医療・介護のデータの有機的な連結に向けた「ICT インフラの抜本改革」や、「ゲノム解析や AI 等の最先端技術の医療への導入」の具体化を実施している本部。
認証局	電子証明書の発行、失効の依頼を受けた電子証明書や秘密鍵の危殆化の可能性のある証明書を失効させる機関。
保険医療機関	保険指定を受けた病院・診療所であり、健康保険を使った診察、処置を行う。
保険薬局	保険指定を受けた薬局であり、健康保険を使った処方箋の受付、調剤を行う。
保健医療福祉分野に	医師資格等の確認機能を備えた電子署名の公開鍵基盤

用語	説明
おける公開鍵基盤認証局の整備と運営に関する専門家会議	（PKI：Public Key Infrastructure）認証局を運営するために準拠すべき「保健医療福祉分野 PKI 認証局証明書ポリシ」について検討している会議体。
保健医療福祉分野 PKI 認証局認証用(組織)証明書	保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議で規定した、保険医療機関、保険薬局を対象とした証明書。
HPKI	Healthcare Public Key Infrastructure。 医師・薬剤師・看護師等、保健医療福祉分野の 26 種類の国家資格と、院長・管理薬剤師等 5 種類の管理者資格を電子的に認証することができると厚生労働省が認めた唯一の公開鍵基盤。
HPKI 準拠性審査	保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議にて、ルート認証局及びサブ認証局を対象に実施している審査。
IPsec	IP レイヤー（ネットワーク層）において暗号に基づくセキュリティサービスを提供する機能。インターネット規格の RFC 4301 で規定。
OID	Object Identifier。オブジェクトクラスまたは属性と一対一に対応するユニークな番号。
Open-VPN	OpenVPN Technologies, Inc. を中心に開発が行われているオープンソースの VPN（Virtual Private Network）ソフトウェア。
PKI	Public Key Infrastructure。インターネット上で安全に情報のやりとりを行うセキュリティのインフラ（基盤）のこと。
TLS1.2	Transport Layer Security 1.2。 セキュリティを要する通信で用いられる、代表的な通信プロトコルの一つ。ハッシュに SHA-256 が追加されたバージョンで、RFC 5246 として標準化された。