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

最終報告書概要版

平成 30 年 3 月 30 日

ジャパンネット株式会社

目次

1. 調査概要

1.1. 本事業の目的

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. 本事業の概要

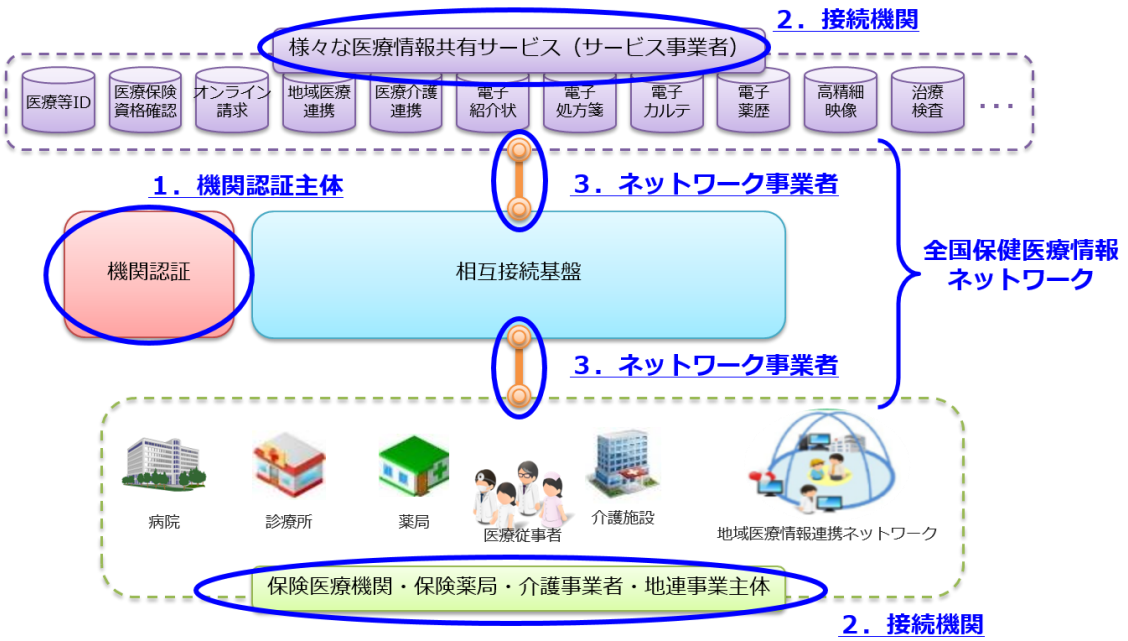
1.2.1. 実施内容

本事業は図表 1-1 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 1-2 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。

図表 1-1　調査研究対象[1]



図表 1-2　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

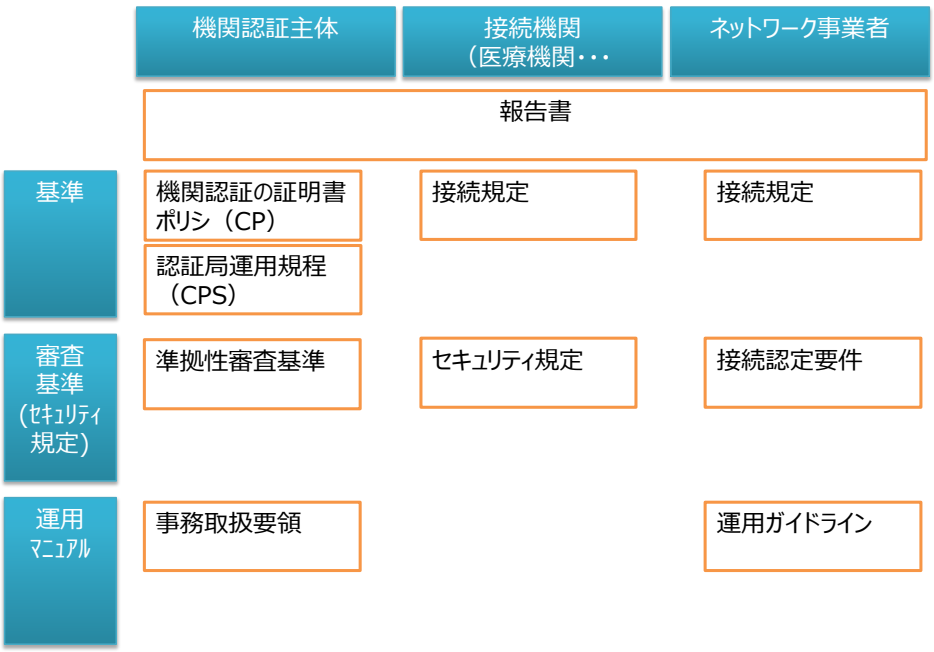
[1]出典：未来投資会議構造改革徹底推進会合「健康・医療・介護」会合（第２回）
厚生労働省・総務省・経済産業省　提出資料「（２）データ利活用基盤の構築」を参考に作成。

#	テーマ	対象	内容
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基に、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 1-3)。

- 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 1-3　本事業の成果ドキュメント

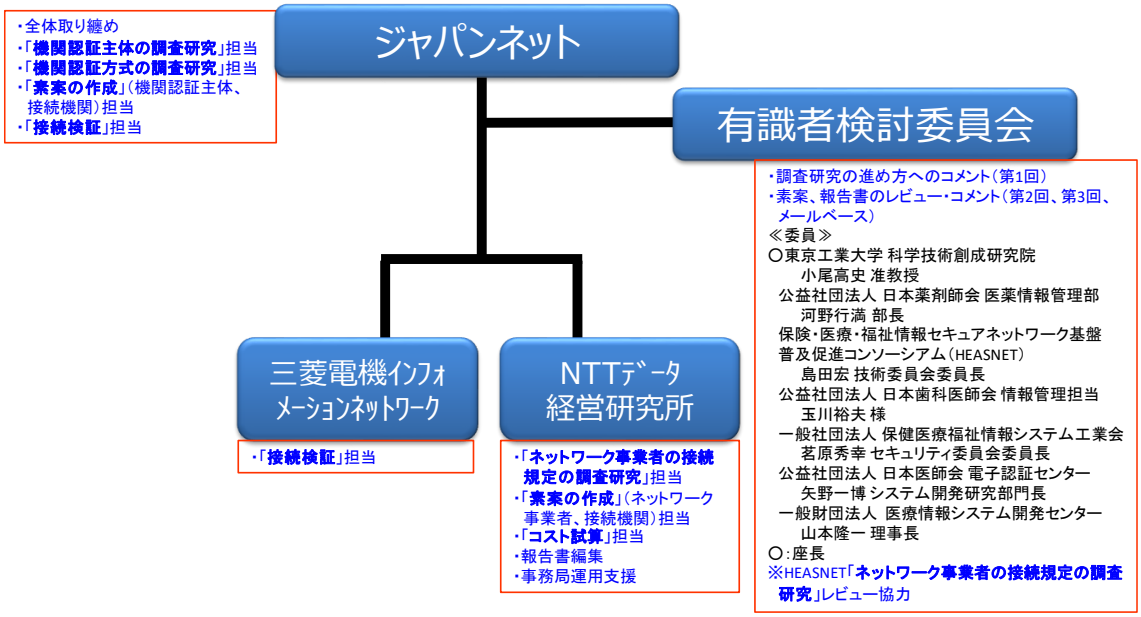


1.2.2. 実施体制

本事業は図表 1-4 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 1-4　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。

1.2.3. 実施スケジュール

本事業は

図表 1-5 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 1-5　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 ・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）	・報告書骨子作成 △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）	・最終報告書作成
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（3/30） △素案 接続機関、ネットワーク事業者（2/28） △最終報告書

2. 調査研究の成果

2.1. 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

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、下記（1）から（7）を実施した。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、機関認証主体向け文書である「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」の素案を作成した。

（1）認証の主体のあり方

機関認証主体となる事業主体、機関認証用証明書の種類、機関認証主体の役割、厚生労働省ルート認証局との接続について検討した。

機関認証主体となる事業主体については、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た。

機関認証用証明書の種類については、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 種類を発行するとした。

機関認証主体の役割については、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とした。

厚生労働省ルート認証局との接続については、厚生労働省ルート認証局との接続は不要とし、ISO 17090 に準拠した独自のルート認証局として「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」の準拠性監査を受けることを要件とした。ま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、構成を特定していない。

（2）認証主体の業務

認証主体の業務のうち、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下記 1)から 6)の業務について検討し詳細化することとした。

1) 接続機関からの発行申請等受付
2) 接続機関の組織の正当性審査
3) 機関認証用証明書の失効
4) 機関認証用証明書の更新（継続）
5) 機関認証用証明書の再発行

検討した結果については、後述の「2.1（4）接続機関の認定基準」「2.2.（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「2.2.（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。

（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
2) 証明書発行
3) 証明書配付

証明書配付時、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。

（４）接続機関の認定基準

本事業が想定する接続機関である、保険医療機関、保険薬局、地連事業主体、介護事業者、サービス事業者の認定基準について検討した。
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。
地連事業主体、サービス事業者の認定基準の認定基準は、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た。

（５）認証主体の運用方法

認証主体の運用方法、機能、体制・役割について検討した。運用の中で、2 年に 1 回「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」による監査（準拠性監査）を受けることとした。

（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を検討し、3 つの方法について整理した。

- 接続機関からの失効申請
  認証局の義務として必ず実施する必要がある。
- 公的機関の公表情報を確認

保険医療機関・保険薬局の場合は地方厚生局のホームページ、介護事業者の場合は都道府県・市町村のホームページや介護サービス情報公表システム、法人の場合は国税庁の法人番号公表サイト、といった公開情報を確認する。

- 第三者との情報連携
  ネットワーク事業者の接続機関へのサービス停止との連携が考えられるが、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必要である。

（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、「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）の見直しを実施し、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」を作成した。さらに見直した結果を基に機関認証用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」を基にしている。

2.2. 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

全国保健医療情報ネットワークに接続する機関を想定し、その認証方法について、下記（１）から（１２）を実施した。機関認証用証明書に記載する情報や、機関認証用証明書の発行対象である接続機関の審査方法、機関認証用証明書の配付方法、失効管理について調査研究を実施し、機関認証主体向け文書である「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」を作成した。

また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、接続機関向け文書である「接続規定」「セキュリティ規定」の素案を作成した。

（１）機関用証明書記載情報（機関用 OID、hcRole(healthcare Role)）

機関認証用証明書の記載情報として、機関用 OID（object identifier、以下 OID)、hcRole、証明書プロファイルについて検討した。

機関用 OID については、厚生労働省が所有する OID「1.2.392.100495」（＝MHLW）から派生することとし、検討を行った。本事業が想定する接続機関の業種毎に分岐し、同一業種内の機関毎の OID や同一業種内の機関毎の OID の枝番を採番することで、OID となる一意性を持たせた。

hcRole については、既に HPKI-CP に組織名が規定されている保険医療機関と保険薬局以外で本事業が想定する接続機関である、地連事業主体、介護事業者、サービス事業者について規定した。

証明書プロファイルについては、証明書の有効期間は 6 年 5 ヶ月を越えないとした。サブジェクト名は機関用 OID を設定する OrganizationalUnitName(OU)を追加した。証明書拡張情報 KeyUsage は WEB サーバ証明書として利用可能となるよう、「KeyEncipherment」をオプション項目として追加した。証明書拡張情報 ExtendedKeyUsage も同様に WEB サーバやクライアント証明書として利用可能となるようオプション項目として追加した。

（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）

指定通知書を確認する保険医療機関・保険薬局・介護事業者と、そうでない地連事業主体、サービス事業者に分けて、審査方法について検討した。

保険医療機関・保険薬局・介護事業者の審査方法については、指定通知書と申請書類の突き合わせや都道府県・市町村・地方厚生局等のホームページを確認することで、実在性と有資格性を確認するよう考えた。

地連事業主体、サービス事業者については、法人の場合は登記事項証明書と申請書類の突き合わせや国税庁法人番号公表サイトを確認することで、実在性を確認するよう考えた。個人の場合は個人事業主であることを証明できる書類を例示し、その書類

と申請書類を突き合わせすることで、実在性を確認するよう考えた。

（３）機関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）

機関認証用証明書の新規発行、更新発行、再発行、失効それぞれにおける審査方法について検討した。

機関認証用証明書の新規発行時の審査は、「2.2（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）」に基づき実施するよう考えた。

更新発行、再発行、失効時の審査も、確実な実在性を担保するため、新規発行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た。

（４）機関用証明書配付方法（オフライン時の対応）

機関認証用証明書のオフラインによる配付方法について、キーペアの生成方法別に検討した。

キーペアを利用者側（接続機関）機器等で生成する場合、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よう考え、接続機関と機関認証主体との間の手順を整理した。

キーペアを機関認証主体（認証局）で生成する場合、機関認証主体は、接続機関からの申請書類情報に基づき、機関認証主体にて公開鍵及びそれに対応した私有鍵（活性化 PIN 含む）、機関認証用証明書を生成し、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よう考え、接続機関と機関認証主体との間の手順に加え、ネットワーク事業者も含めた手順を整理した。

（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。

（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

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、紐付けが必要となる場面を想定し考察した。

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が、TLS 通信であればネットワーク事業者が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。

（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、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」を作成した。

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」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」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

（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した。

検討の結果、運用方法の案として、ネットワーク事業者にてモバイル端末かどうかを確認して適切なアクセス制御を行う方法が考えられた。

（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と考えた。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ことが分かった。

このため、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、本事業の作成ドキュメントである「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。

（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」を参考に以下のケースにおける認証方法を調査した。

1) 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
2) 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

調査した結果、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 PKI 認証を実装する場合の要件を以下の通り整理した。

- トラストアンカの適切な設定と管理
- 機関認証用証明書の公開鍵を用いた署名の検証
- 機関認証用証明書の認証パスの有効性確認
- 「サブジェクト名」属性の取得
- 「hcRole」属性の取得

また、上記以外の機関認証用証明書を用いる場合の留意事項や外部利用者認証システムを利用する場合の留意事項を整理した。

（１１）IPsec VPN、SSL-VPN、Open-VPN など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

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の検討として、「IPsec-VPN」と「Open-VPN（SSL-VPN の一種)」を対象に調査した。

調査した結果、機能性においては IPsec-VPN と Open-VPN に大きな差異はないと考えられた。しかし Open-VPN については、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た。

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た。

（１２）接続機関の規定

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、本事業の作成ドキュメント「セキュリティ規定」「接続規定」である。

セキュティ規定については、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した。考察にあた

り、接続機関を下記の 2 つの役割に分類した。

1) 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。

2) 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。

考察した結果、セキュリティ基準の審査方法については、以下の通り整理した。

- リクエスタの審査方法
  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（自己申告）。
- レスポンダの審査方法
  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（第三者評価）。

接続規定については、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した。考察した結果、接続方式については、以下の通り整理した。

- 保険医療機関、保険薬局、介護事業者の接続方式
  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、サービス事業者の接続方式
  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」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。

2.3. ネットワーク事業者の接続規定

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、接続認定のためのセキュリティ基準、運用要件について、下記（1）から（4）を実施した。この調査結果を基に、ネットワーク事業者向け文書である「接続規定」「接続認定要件」「運用ガイドライン」の素案を作成した。

（1）既存ネットワークの接続方式

ネットワーク事業者のネットワーク接続方式として選択可能なものを、「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」に記載の方式の中から考察した。考察した結果、接続方式については、以下の通り整理した。

- 相互接続基盤との接続方式
  IP-VPN 接続サービス
  専用線接続サービス
- 接続機関との接続方式
  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」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。

（2）暗号化要件

ネットワーク接続方式毎に暗号化要件を整理した。

- 専用線接続サービス
  一般的には暗号化は不要
- IP-VPN 接続サービス
  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
- インターネット VPN（IPsec+IKE）接続サービス
  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る

（３）接続認定要件

ネットワーク事業者を認定する要件として、組織の実在性、組織の申請意思、セキュリティ基準準拠について整理した。

組織の実在性の要件は、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とした。組織の申請意思の要件は、申請する組織の責任者が申請をしていることとした。セキュリティ基準準拠の要件は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」を準拠することとした。

さらにそれぞれの確認方法を整理した。組織の実在性の確認方法は、提出された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）を総務省のホームページに掲載されている事業者の一覧から確認することとしたが、一部の事業者（電気通信事業法第 16 条第１項の規定による届出をした者）は一覧がホームページに掲載されていないため、確認方法については今後さらに検討が必要である。組織の申請意思の確認方法は、申請書類等への責任者署名・押印を確認することとした。セキュリティ基準準拠の確認方法は、相互接続基盤の事業主体による審査（直接確認）、または相互接続基盤の事業主体が認定（信頼）した第三者機関による審査（第三者確認）を受けることとした。

（４）運用要件

運用要件は以下の３つに分けて検討し、本事業の「運用ガイドライン」を作成した。

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
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

ネットワーク事業者における運用要件については、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として、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。

ネットワーク事業者と接続機関間における運用要件については、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」を規定することとした。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の手順の整理や、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。

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については、ネットワーク監視、障害発生時における報告方法を検討した。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。

2.4. コスト試算

「2.1 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」「2.2 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」「2.3 ネットワーク事業者の接続規定」での調査研究を基に、機関認証の認定、認証にかかるイニシャルコスト、運用コストについて、下記（1）から（3）の試算を実施した。

（1）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）

認証局のシステム構成として図表 2-1 の通り 3 パターン設定し、それぞれの初期費用を図表 2-2 の通り算出した。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。

図表 2-1　認証局のシステム構成の設定[2]

構成	認証局機能
A（梅）	オフライン証明書申請 オフライン証明書配付 →シングル構成
B（竹）	オフライン証明書申請 オンライン証明書配付 →冗長構成
（参考） C（松）	オンライン証明書申請 オンライン証明書配付 →冗長構成

図表 2-2　システム構成パターン別の初期費用

構成	1ヶ月あたりの発行枚数（枚）	初期費用（円）
A（梅）	750　（1 年・9,000、6 年・54,000）	123,900,000
	1,500　（1 年・18,000、6 年・108,000）	125,700,000
B（竹）	750　（1 年・9,000、6 年・54,000）	200,700,000
	1,500　（1 年・18,000、6 年・108,000）	202,500,000
（参考） C（松）	750　（1 年・9,000、6 年・54,000）	247,000,000
	1,500　（1 年・18,000、6 年・108,000）	247,400,000

[2] 下線はパターンB（竹）の場合にパターン A（梅）に追加される機能・業務・効果を指す。二重下線はパターン C（松）の場合に追加される機能・業務・効果を指す。

（２）運用費用（設備維持費用、人件費等）

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。試算結果は図表 2-3 通りとなる。

図表 2-3　システム構成パターン別の設備維持費・人件費（月額）

構成	１ヶ月あたりの発行枚数（枚）	設備維持費（月額・円）	人件費（月額・円）
A（梅）	750　（1 年・9,000、6 年・54,000）	3,700,000	10,620,000
	1,500　（1 年・18,000、6 年・108,000）	3,900,000	18,300,000
B（竹）	750　（1 年・9,000、6 年・54,000）	5,700,000	9,220,000
	1,500　（1 年・18,000、6 年・108,000）	5,900,000	15,500,000
（参考）C（松）	750　（1 年・9,000、6 年・54,000）	6,000,000	5,080,000
	1,500　（1 年・18,000、6 年・108,000）	6,000,000	7,220,000

（３）証明書発行１枚あたりの費用

初期費用及び 6 年間の運用費用の試算結果は図表 2-4 の通りとなる。

図表 2-4　初期費用・運用費用（6 年間）の試算結果

構成	１ヶ月あたりの発行枚数（枚）	6 年間の総費用（円）
A（梅）	750　（1 年・9,000、6 年・54,000）	1,316,940,000
	1,500　（1 年・18,000、6 年・108,000）	2,048,100,000
B（竹）	750　（1 年・9,000、6 年・54,000）	1,350,540,000
	1,500　（1 年・18,000、6 年・108,000）	1,894,500,000
（参考）C（松）	750　（1 年・9,000、6 年・54,000）	1,093,360,000
	1,500　（1 年・18,000、6 年・108,000）	1,296,440,000

6 年間の総費用を踏まえて、証明書発行１枚あたりの年間費用を試算した。

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 2-5　証明書１枚あたりの年間費用に示す。効率的な審査・発行が可能な構成 B 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、構成 B・C においては 2,000 円～4,000 円程度となる。

また、実運用では医療機関等に複数枚の証明書を発行する場合は、審査費用は１回

となるため、証明書１枚あたりの費用はより安価に提供することが可能となる。

図表 2-5　証明書１枚あたりの年間費用

構成	１ヶ月あたりの発行枚数（枚）	１枚あたりの年間費用（円）
A（梅）	750　（1 年・9,000、6 年・54,000）	4,065
	1,500　（1 年・18,000、6 年・108,000）	3,161
B（竹）	750　（1 年・9,000、6 年・54,000）	4,168
	1,500　（1 年・18,000、6 年・108,000）	2,924
（参考）C（松）	750　（1 年・9,000、6 年・54,000）	3,375
	1,500　（1 年・18,000、6 年・108,000）	2,001

2.5. 接続検証

本調査研究で策定した準拠性審査基準に適合する環境においてテスト証明書を発行し、ネットワークレベルの機関認証用証明書による接続検証として、下記（1）を実施した。ま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）の接続検証として、下記（2）を実施した。

検証の結果、ネットワークレベル、アプリケーションレベルともに、「2.2 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」で検討した情報を記載した機関用証明書を用いて接続できることが確認できた。

（1）IPsec+IKE 方式による VPN 接続検証

検証用に作成した証明書を用いて、失効確認を含めた証明書検証を実施した VPN 接続を確認することができた。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、SubjectDirectoryAttributes に記載の hcRole を用いて接続を制御ができなかった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、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

検証用に作成した証明書を用いて、失効確認を含めた証明書検証を実施した TLS1.2 方式によるサーバ認証／クライアント認証の HTTPS 接続を確認することができた。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、Subject-OrganizationUnitName に記載の機関用 OID を用いて接続を制御ができなかったことや、SubjectDirectoryAttributes に記載の hcRole を用いた接続の制御やログに機関用 OID を記録する試験が実施できなかった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。

3. 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。

3.1. 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「2.1.（４）接続機関の認定基準」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・Ｓａａ Ｓ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「2.4 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。

3.2. 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「2.4 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「2.4 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「3.1.（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「3.1.（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。