31 東広総総第 985-2 号
令 和 2 年 1 月 17 日

東京都後期高齢者医療広域連合
情報公開・個人情報保護審議会会長　様

東京都後期高齢者医療広域連合長
山﨑　孝明

令和元年度諮問第５号

東京都後期高齢者医療広域連合情報公開・個人情報保護審議会条例第２条に基づき下記の事項について諮問します。

記

１　電子計算組織の結合の可否について

更改後の医療保険者等向け中間サーバー等への接続について

審議会資料
令和2年１月31日
保険部管理課

更改後の医療保険者等向け中間サーバー等への接続について

1　件名

別紙「電算結合記録票」のとおり

2　電算結合内容

現在、取りまとめ機関（社会保険診療報酬支払基金（以下、「支払基金」という。）及び国民健康保険中央会（以下、「中央会」という。））に管理・運用を委託している医療保険者等向け中間サーバー等（以下、「中間サーバー」という。）の機器更改に伴い、新中間サーバーとの接続を行う。なお、新中間サーバーではオンライン資格確認等システムとも接続する。

新中間サーバー及びオンライン確認等システムはＡ社（クラウド事業者）が提供するクラウド方式を利用する。契約によりＡ社は個人情報を取扱わないこととし、アクセス制御を行う。

3　理由

マイナンバー情報連携業務に使用している中間サーバーについては、現在、取りまとめ機関に管理・運用を委託している。このたびの取りまとめ機関で中間サーバーの機器更改に伴い、更改後の中間サーバーに接続する必要があるため。

4　個人情報保護・安全対策

(1) クラウドサービスの安全対策について

新中間サーバーの運用は、従前どおり取りまとめ機関が行う。取りまとめ機関ではクラウドサービスの利用にあたり、以下のように定めている。

ア　国内法に基づいた対応をとること

国内法に基づいた対応をとるため、クラウドサービスに以下の要件を定めている。

（ア）データセンターの物理的所在地が日本国内であること。

（イ）発注者の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。

（ウ）障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンターに移管されないこと。

(ア)～(ウ)について、本クラウドでは国内において東京及び大阪の拠点があり、サービスの利用は東京、バックアップのため大阪拠点のみデータ移管を許可する設定としている。データ移管や操作といった履歴はログに記録され、確認することができる。

なお、ストレージデバイスが製品寿命に達した場合は NIST800-88（記録媒体のデータ消去、廃棄における規格）に則りメディアを廃棄する。廃棄プロセスは ISO27001 により保証されている。

（エ）クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方

裁判所を専属的合意管轄裁判所とするものであること。

(オ) 契約の解釈が日本法に基づくものであること。

(エ)～(オ)について、本クラウドでは契約により準拠法を日本法とし、東京地方裁判所を専属的管轄裁判所としている。

(カ) 法令や規制に従って、クラウドサービス上の記録を保護すること。

(キ) 自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知すること。クラウドサービスを利用する際、コンテンツの所有権と管理権はユーザーが保有し続けることとしている。

イ　不正アクセスの防止

サービスを提供するシステムが二以上の部分から構成され、かつ、電気通信回線を介して複数の建物間で送受信される場合は、一方から他方への通信に関し、送信した設備の誤認並びに通信内容の盗聴及び改変を防止する仕組みを備えること。

ウ　設置場所の入退場管理

サービスを提供するシステムが、ID カード等による入退場管理を行う部屋に設置されること。他システムを同じ部屋に設置する場合は、搭載するサーバーラックを分けた上でサーバーラックに対する施錠等の手段により、関係者以外がサービスを提供するシステムに触れることできないよう措置を講じること。

エ　第三者認証の取得

クラウドサービス事業者は、セキュリティに係る情報の収集・対策の向上を常に実施しており、以下の第三者認証を取得している。

(ア) ISO27017

クラウドベースの情報セキュリティの統制。国際標準化機構（ISO）は独立した非政府国際組織による認証。

(イ) SOC2

セキュリティ、可用性、機密保持に関する統制。セキュリティ、可用性、処理の整合性、機密性保持、プライバシーなどに関して重要なコンプライアンス管理および目標をどのように達成したかを実証する、独立したサードパーティーによる審査報告書。

(ウ) CS ゴールドマーク

クラウドサービスプロバイダーを対象としたセキュリティ基準。情報セキュリティコントロールの国際実施基準である ISO/IEC 27017 に基づく。総務省と経済産業省が設立した非営利法人、日本セキュリティ監査協会（JASA）による認証。

(2) 通信回線の安全対策

以下の通信回線を利用することで、通信内容秘匿、盗聴防止の対応をしている。

ア　東京都後期高齢者医療広域連合から NTT 東日本のネットワーク機器まで

IP-VPN（閉域通信サービス。他の利用者と論理的に分離している。）を利用する。

イ　NTT 東日本ネットワーク機器から新中間サーバーまで

通信事業者が設置した専用回線を利用する。

5　付議希望日

　令和元年度第３回審議会

6　その他

＜事由等が明らかになる参考資料を添付＞

(1) 新中間サーバー等への電算結合について（資料１）

(2) システム全体構成図（オンライン資格確認等システム）（参考）

オンライン資格等システムの運用委託について、今後、審議会に諮る予定。

別記第6号様式(第9条関係)

電算結合記録票

令和２年１月　日

業務登録番号	
主管課名	保険部管理課
業務の名称	更改後の医療保険者等向け中間サーバー等への接続
電算結合の目的	マイナンバー情報連携で使用している医療保険者等向け中間サーバー等（以下、「中間サーバー」という。）については、取りまとめ機関（社会保険診療報酬支払基金及び国民健康保険中央会）に管理・運用を委託しているが、このたびの中間サーバーの機器更改に伴い、更改後の中間サーバーに電算結合する必要があるため。
結合年月日	令和２年６月１５日(審議会　年　月　日　諮問第　号)
結合変更年月日	年　月　日(審議会　年　月　日　諮問第　号)
電算結合の相手方	取りまとめ機関 （社会保険診療報酬支払基金及び国民健康保険中央会）
提供する保有個人情報又は提供を受ける個人情報の記録の項目	・基本的事項(氏名、住所、生年月日、続柄など) ・経済活動(収入、財産、納税額、負債状況、公的扶助など) ・心身健康(健康状態、病歴、障害など) ・マイナンバー及び被保険者枝番

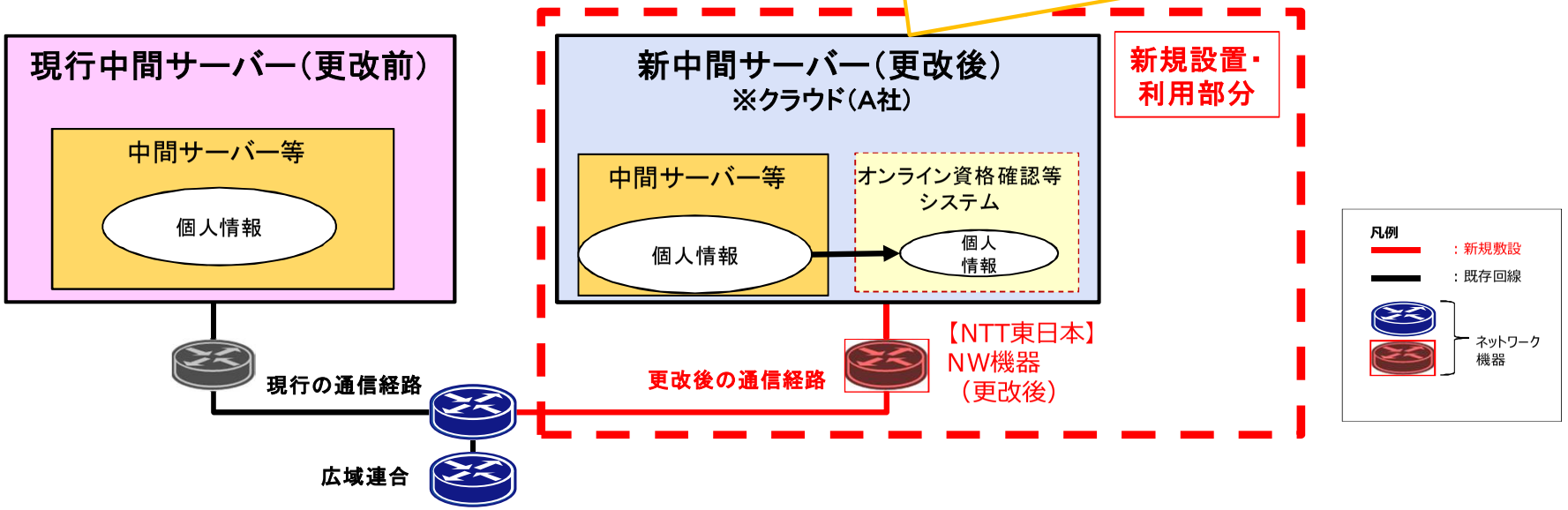
(用紙規格　A4)

新中間サーバー等への接続について　[電算結合内容]

資料1-1

【諮問事項】
・中間サーバーの機器更改に伴い、新中間サーバーに接続する。

・新中間サーバーはオンライン資格確認等システムと連携する。（マイナンバーを除く必要な情報のみを連携）



現行中間サーバーと新中間サーバーの運用等比較

	現行中間サーバー	新中間サーバー	＜参考＞オンライン資格確認等
個人情報の保有者	広域連合（医療保険者）	広域連合（医療保険者）	広域連合（医療保険者）
システム運用	取りまとめ機関 （支払基金・中央会）	取りまとめ機関 （支払基金・中央会）	取りまとめ機関 （支払基金・中央会）
ハードウェア構築	取りまとめ機関 （支払基金・中央会）	A社のクラウド※	A社のクラウド※
データセンター構築	取りまとめ機関 （支払基金・中央会）	A社のクラウド※	A社のクラウド※
接続する回線	専用回線	専用回線	専用回線

※　A社（クラウド事業者）は個人情報を扱わない。

取りまとめ機関（社会保険診療報酬支払基金及び国民健康保険中央会）提供資料より作成

新中間サーバー等への接続について ［個人情報保護・安全対策］

資料1-2

（1）クラウドサービスの安全対策
・A社は契約により個人情報を取扱わず、機器の管理を行う。

・データセンターは日本国内に所在し、情報資産は海外に移転されない。また、契約により日本法に準拠することを定めている。

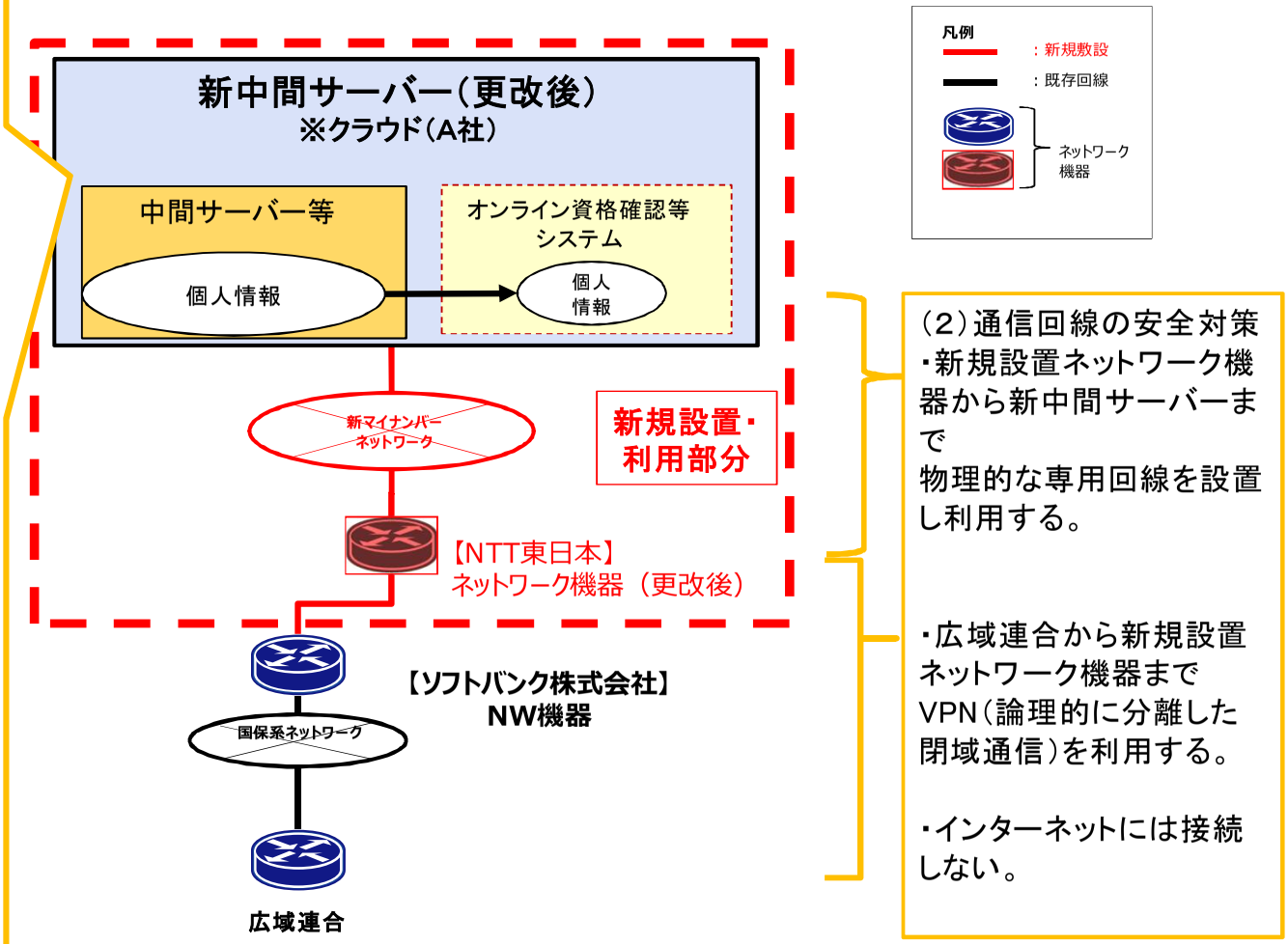
・法令や規制に従って、クラウドサービス上の記録を保護することを要件としている。

・コンテンツの所有権と管理権はユーザーが保有し続けることと定めている。

・記録媒体の廃棄時は規格（NIST800-88）に則り廃棄を行う。

・設置場所のIDカード等による入退場管理（他システムと同じ部屋に設置する場合はラックに施錠）により関係者以外の取扱いを防ぐ。

・ISO27017（クラウド情報管理について）、SOC2（セキュリティ、可用性、機密保持について）、CSゴールドマーク（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）といった第三者認証機関の認証を取得している。



（2）通信回線の安全対策
・新規設置ネットワーク機器から新中間サーバーまで
物理的な専用回線を設置し利用する。

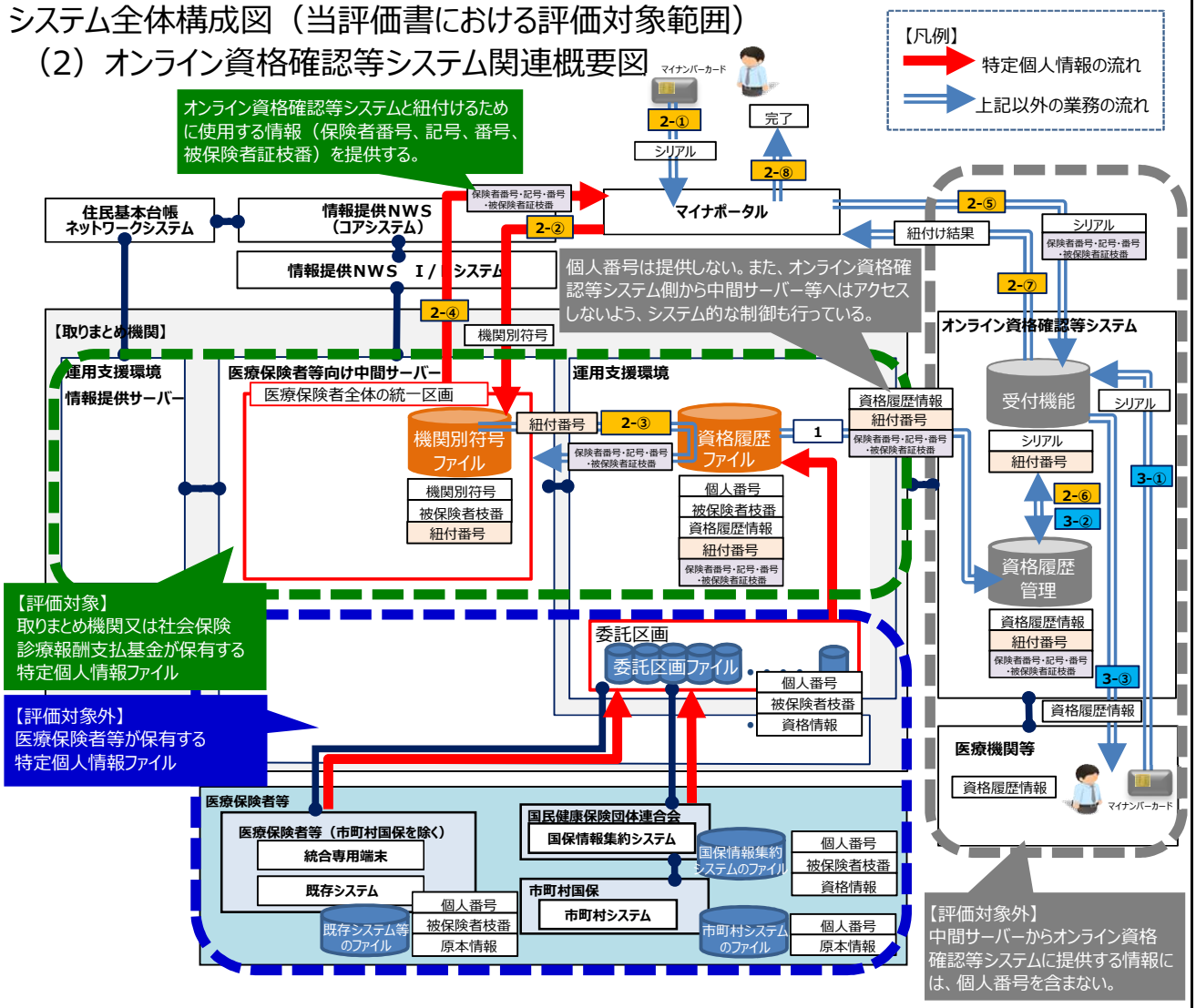
・広域連合から新規設置ネットワーク機器まで
VPN（論理的に分離した閉域通信）を利用する。

・インターネットには接続しない。

取りまとめ機関（社会保険診療報酬支払基金及び国民健康保険中央会）提供資料より作成

（別添1）事務の内容

システム全体構成図（当評価書における評価対象範囲）
（2）オンライン資格確認等システム関連概要図



（備考）

医療保険者等向け中間サーバー等とオンライン資格確認等システムの関連業務は、以下のとおり。
なお、「1」及び「3」の業務については、個人番号を含まないため、本評価書での評価対象外とする。

1.オンライン資格確認等システムへの資格履歴情報の提供
医療保険者等向け中間サーバー等からオンライン資格確認等システムに提供する情報には、個人番号を含まない。また、オンライン資格確認等システム側から医療保険者等向け中間サーバー等へはアクセスしないよう、システム的な制御を行う。

2.オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供
オンライン資格確認等システムと紐付けるために使用する情報（保険者番号、記号、番号、被保険者証枝番）をマイナポータルへ提供する。

3.医療機関等の窓口での資格確認
医療機関等の窓口からオンライン資格確認等システムに接続し、資格履歴情報を確認する。