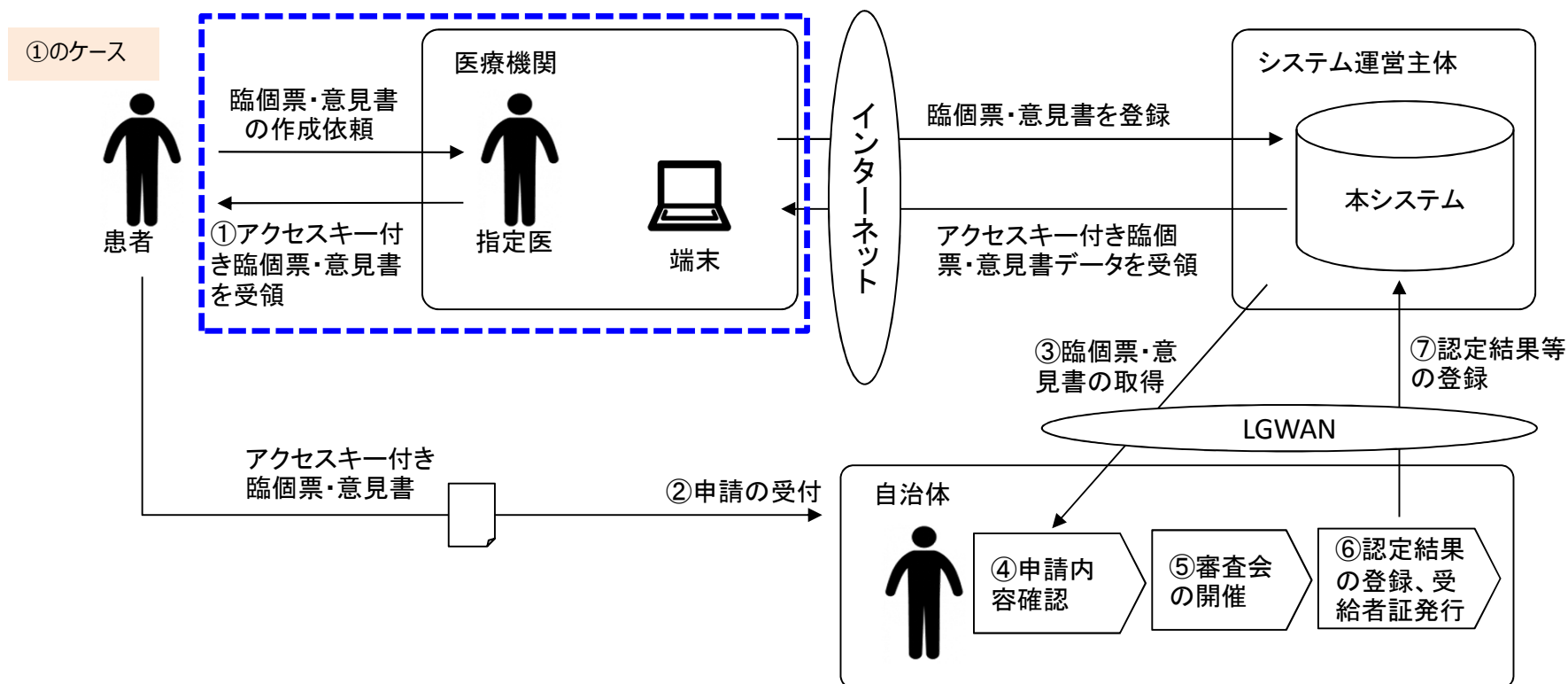


參考資料

オンライン化後の医療費助成の申請とデータ登録の流れ①（イメージ）

- 新システム稼働後では、以下2通りの患者からの申請が発生することとなる。
 - ①指定医が新システムを用いて臨個票・意見書を作成し、患者が申請するケース
 - ②指定医が新システムを用いず従来通りに臨個票・意見書を作成し、患者が申請するケース

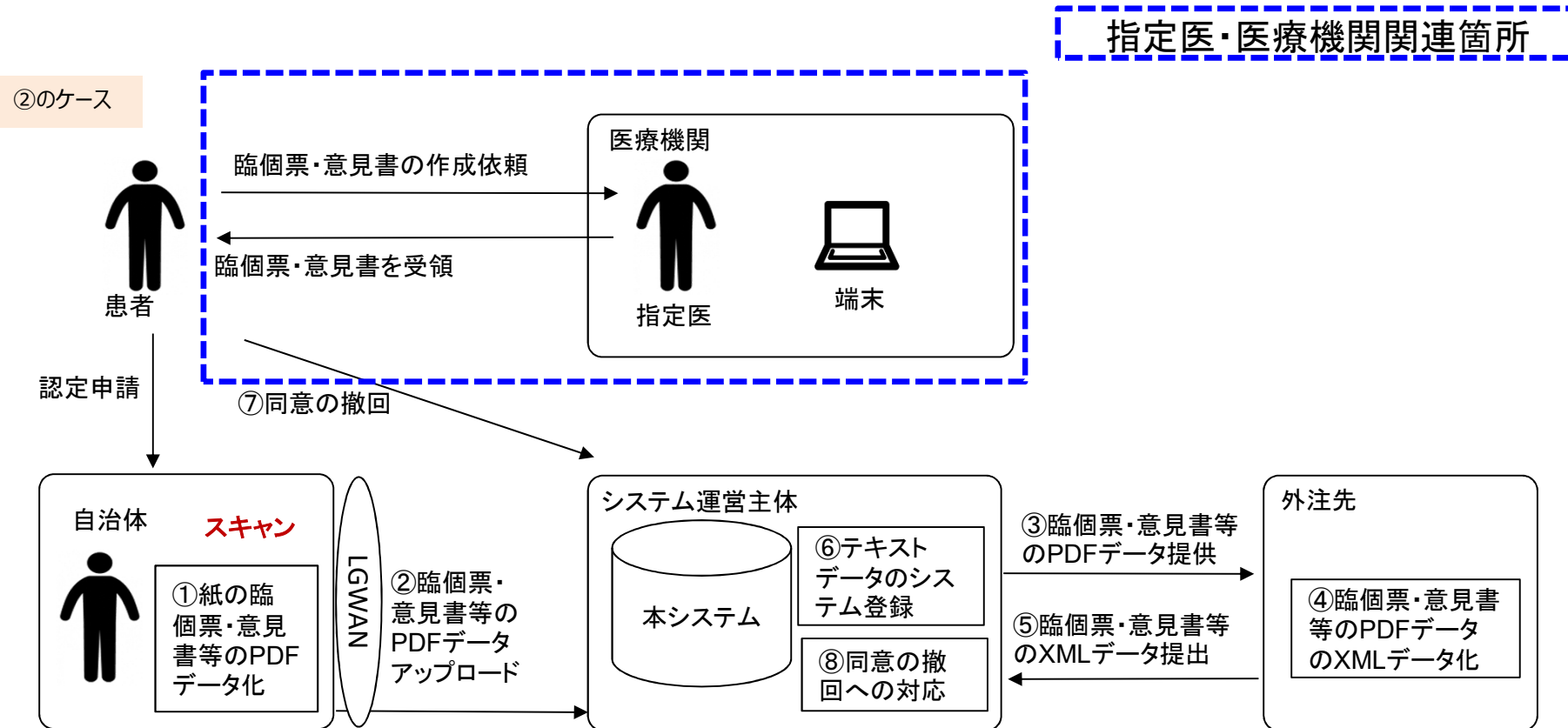
指定医・医療機関関連箇所



- ✓ 指定医にて新システムに臨個票・意見書データを登録し、アクセスキー付き臨個票・意見書を患者に発行する。
- ✓ 申請を受けた自治体では、アクセスキーにより臨個票・意見書の電子データを参照し、新システムの機械判定機能による認定情報を確認できる。これにより、今まで自治体職員が読み込んで判定した業務の負担軽減が期待できる。また、審査会で使用する臨個票・意見書は個人情報をもスキングした状態で新システムよりプリントアウトできる。
- ✓ 自治体では、臨個票・意見書の紙の郵送の手間が削減されるものの、新システムに認定結果、研究利用の同意有無、所得区分等を登録することが必要になる。

オンライン化後の医療費助成の申請とデータ登録の流れ②（イメージ）

- 新システム稼働後では、以下2通りの患者からの申請が発生することとなる。
 - ①指定医が新システムを用いて臨個票・意見書を作成し、患者が申請するケース
 - ②指定医が新システムを用いず従来通りに臨個票・意見書を作成し、患者が申請するケース

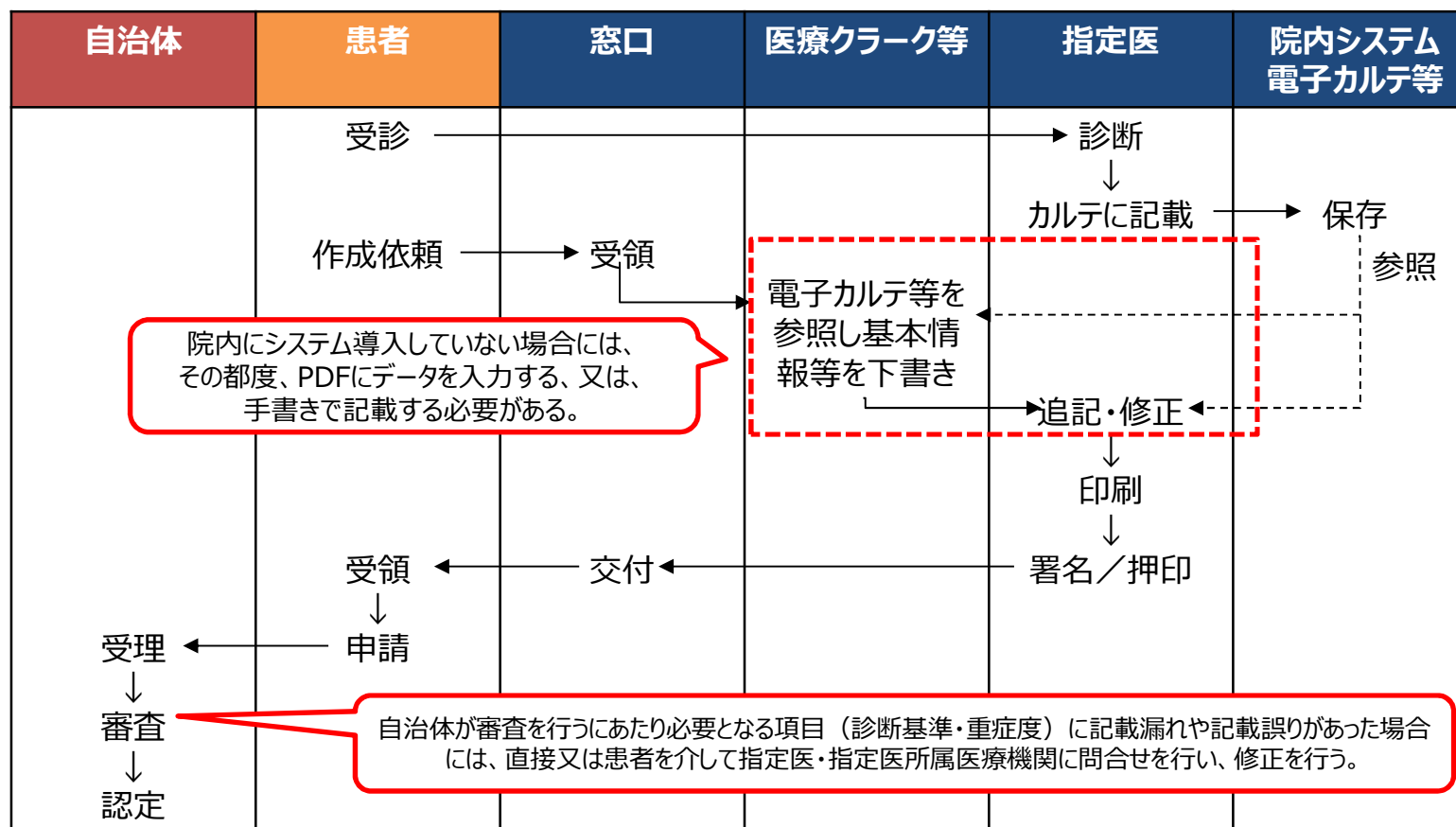


- ✓ 従来通りの紙の臨個票・意見書は、自治体にてスキャンしてPDFデータをファイルサーバにアップロードすることで、システム運営主体へ連携する（郵送は行なわない）。その後、外注先においてXMLデータに変換し、新システムに取り込むことを想定する。

現在の臨床調査個人票・医療意見書作成の流れ（イメージ）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 現在、臨床調査個人票・医療意見書については、毎年、全ての項目について入力又は記載を行う必要があり、指定医等の負担が大きい。
- また、自治体の審査において形式的な誤りが見つかった場合には、その都度、指定医・指定医所属医療機関に確認の上、修正を行う必要があり、自治体・指定医・指定医所属医療機関（場合によっては患者も）にとって、やりとりにかかる負担が大きい。

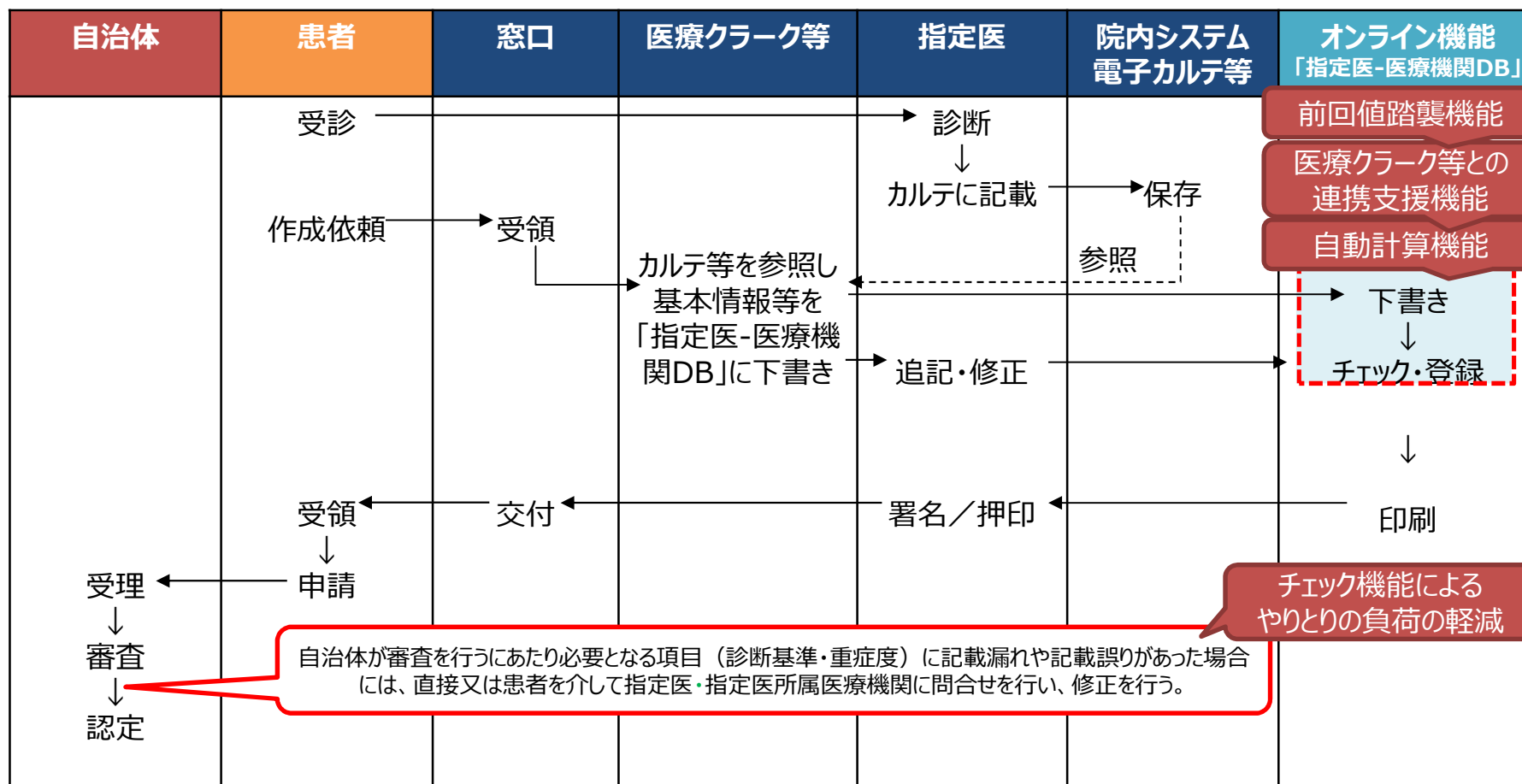


オンライン化後の臨床調査個人票・医療意見書作成の流れ（イメージ）

（パターン1：オンラインにより直接入力を行う場合）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 院内システムがない場合など、オンラインにより直接入力を行う場合には、医療クラーク等が直接、オンライン機能を活用してデータを入力する。指定医がそれを確認・追記修正等した上で、臨個票の内容を確定させ印刷を行うことを想定。また、印刷されたものについて、指定医が最終確認の上、署名・捺印等を行うことを想定。
- オンラインシステム上のチェック機能の活用により、形式的な誤りの軽減を図り、自治体からの問合せの軽減を図る。



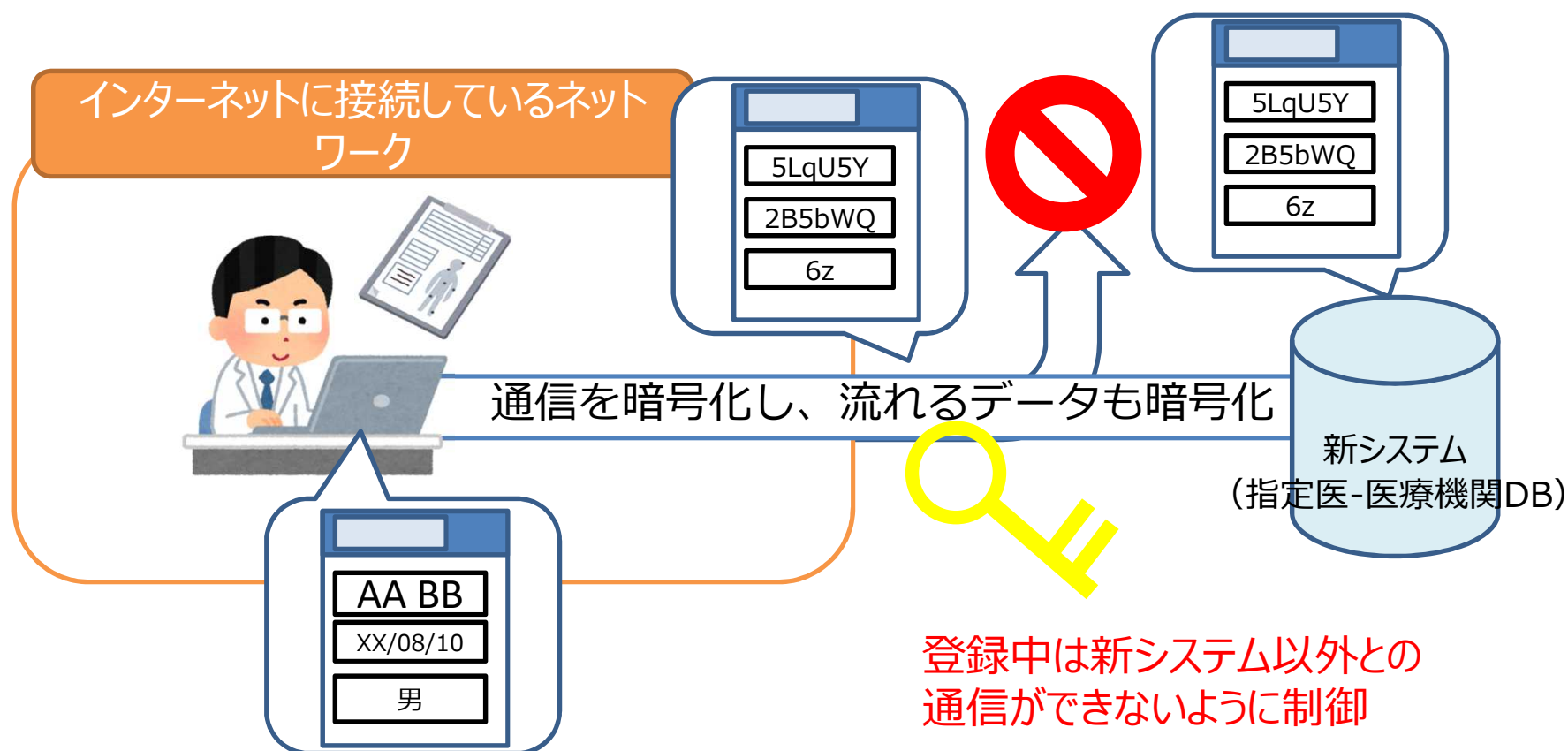
: オンライン上で発生する作業

オンライン化後の臨床調査個人票・医療意見書作成の流れ（イメージ）

（パターン1：オンラインにより直接入力を行う場合）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 「院内システムがない場合などオンラインにより「指定医-医療機関DB」に直接入力を行う場合」においては、紙のカルテ等を参照し、インターネットに接続している端末から直接、新システム（「指定医-医療機関DB」）へアクセスし登録を行う。
- その際、通信を暗号化し通信接続の安全性を確保するとともに、通信経路上を流れるデータについても暗号化することで二重の暗号化を実施する。
- 加えて、接続中は、新システム以外との通信ができないよう制御する。

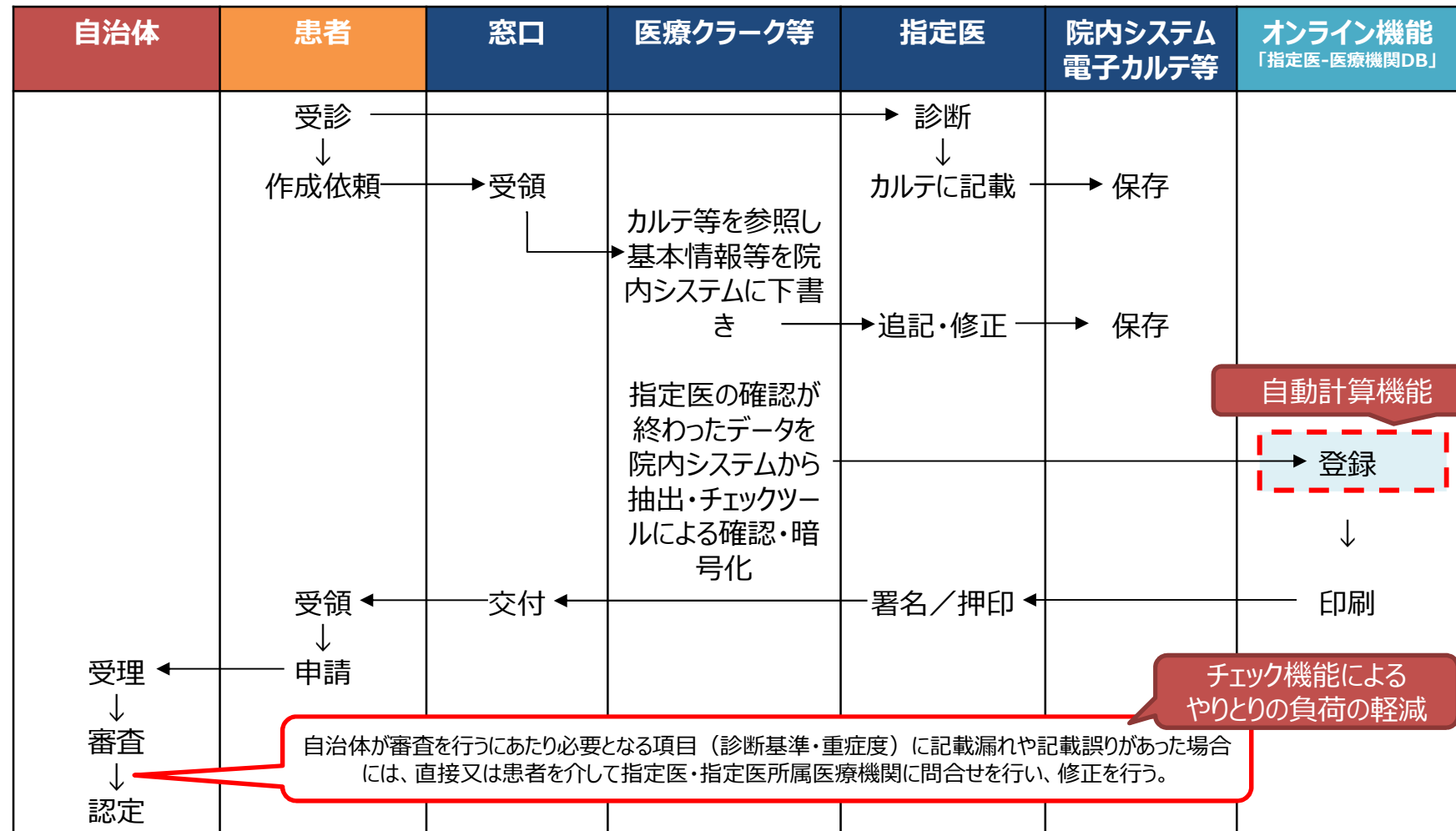


オンライン化後の臨床調査個人票・医療意見書作成の流れ（イメージ）

（パターン２：院内システムで臨個票を作成した上で登録を行う場合）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 既存の院内システムがある場合には、院内システムにて入力を行ったデータを抽出し、配布するチェックツールにおいてチェック・暗号化を行い、一括登録を行う。



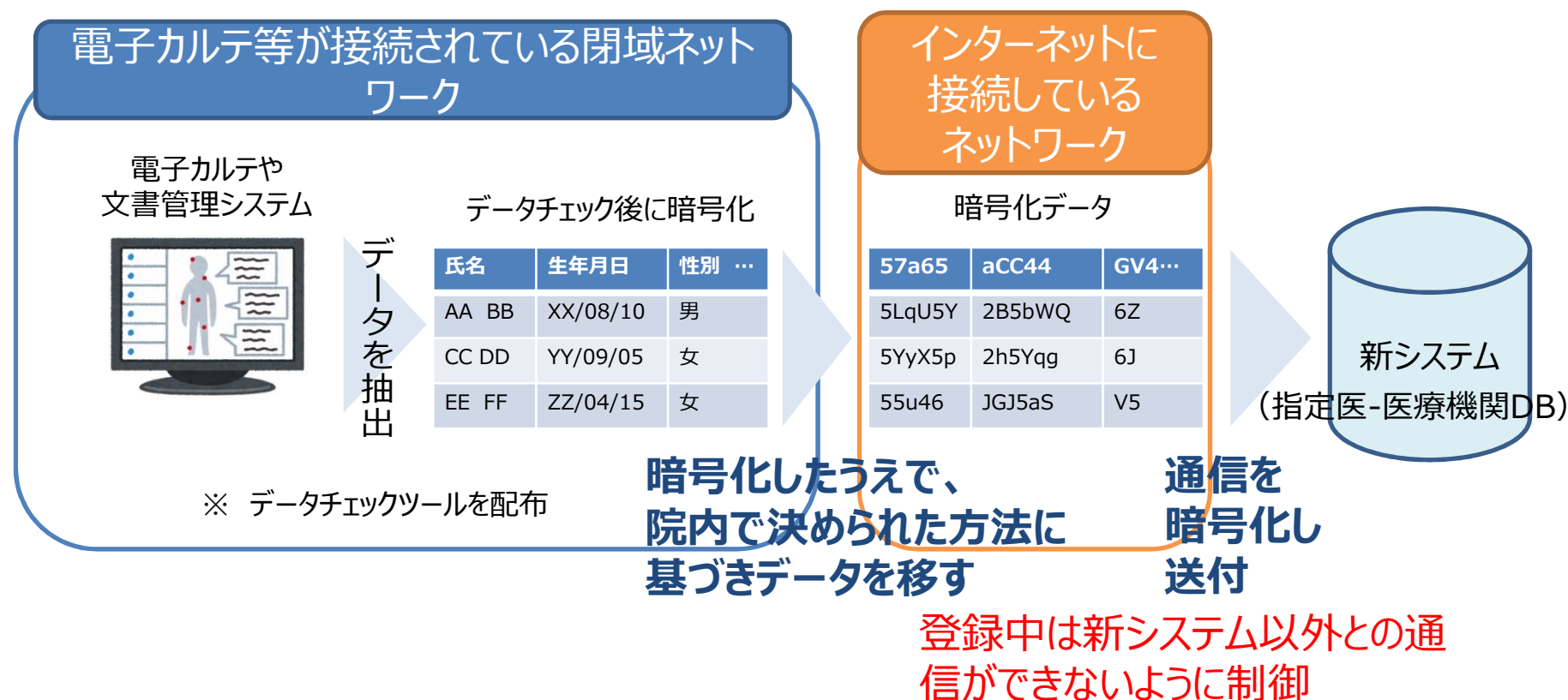
登録：オンライン上で発生する作業

オンライン化後の臨床調査個人票・医療意見書作成の流れ（イメージ）

（パターン2：院内システムで臨個票を作成した上で登録を行う場合）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 「院内システムを活用して臨個票を作成した上で「指定医-医療機関DB」に登録を行う場合」には、まずは、外部と接続していない閉域ネットワーク内で電子カルテや文書管理システム等にデータを入力。
- 厚生労働省が配布予定のチェックツールを用いて、データチェック・暗号化を行い、当該データをセキュリティの確保されたネットワーク※や記録媒体を介して、インターネットに接続している端末へ移す。
※「医療情報システムの安全管理に関するガイドライン」を遵守していることが前提
- そのうえで、暗号化された通信を使って、オンラインでの登録を行う。



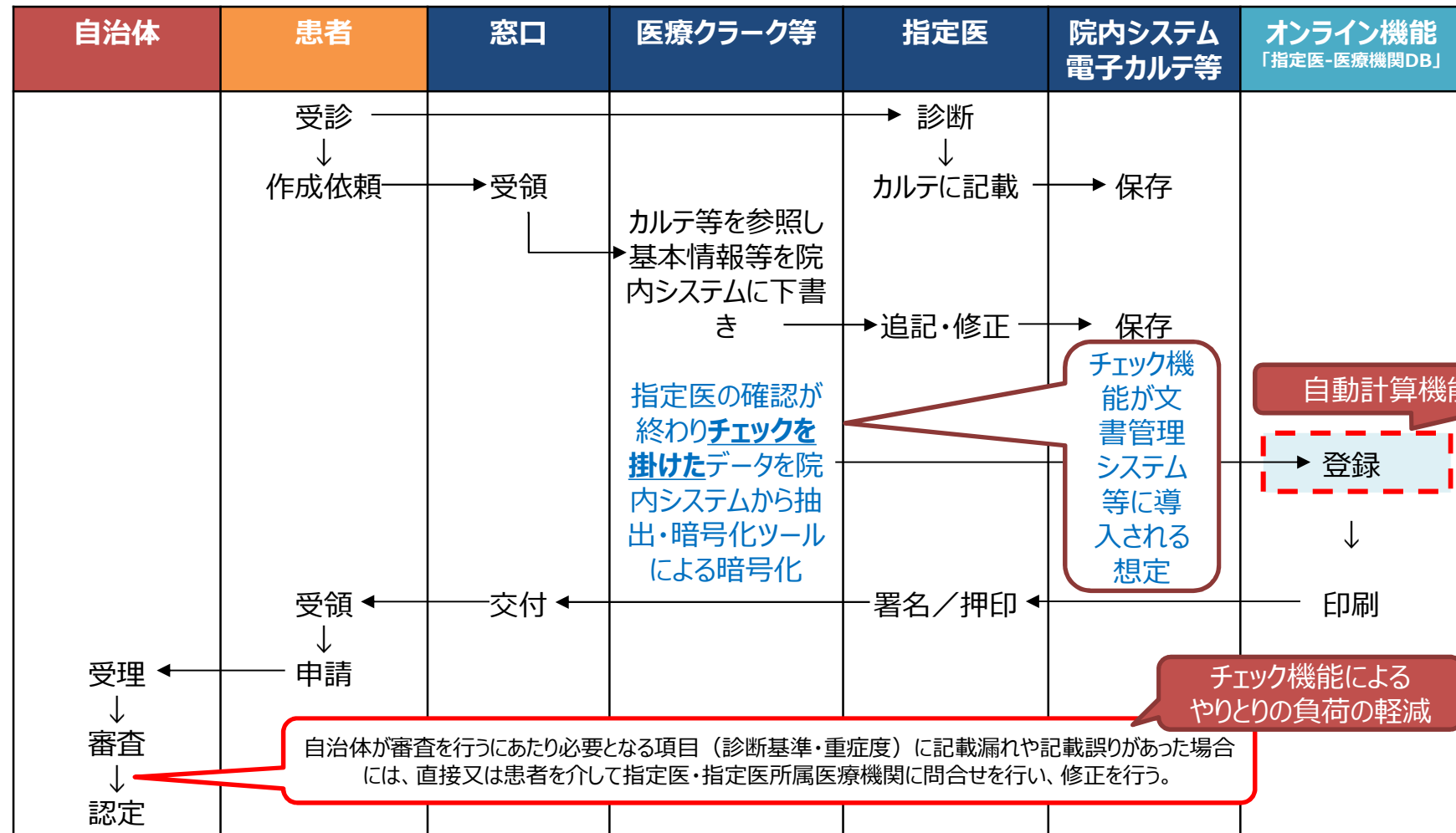
オンライン化後の臨床調査個人票・医療意見書作成の流れ（イメージ）

（パターン3：院内システムで臨個票を作成した上で登録を行う場合）

※パターン2から青字のみ変更

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- 既存の院内システムがある場合には、**院内システムにて入力及びチェックを行ったデータを抽出し、配布する暗号化ツールにおいて暗号化を行い、一括登録を行う。**



登録：オンライン上で発生する作業

補足：がん登録オンラインシステムにおけるセキュリティ対策

難病・小慢 合同委員会
R2. 10. 16 資料1-2 抜粋

■ 安全な通信の仕組み

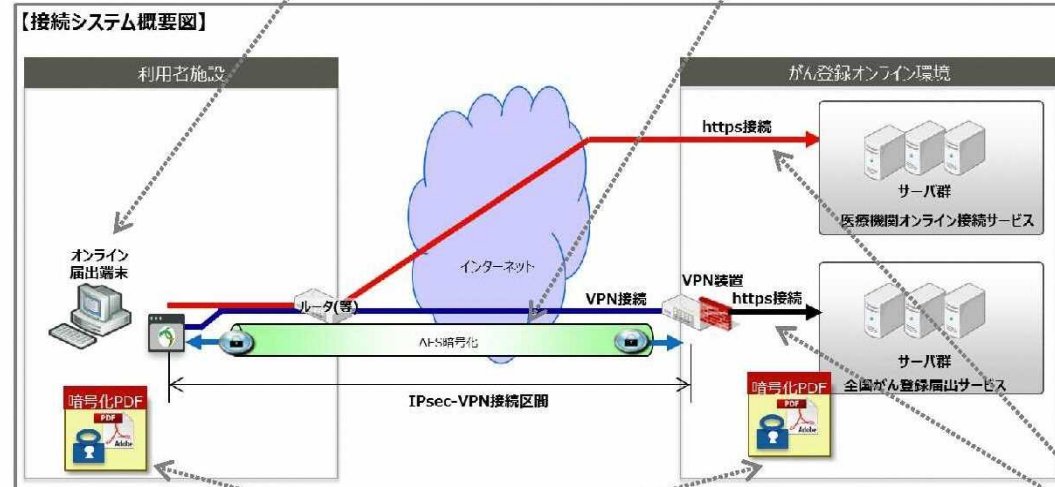
がん登録オンラインシステムでは、機微な情報を取り扱うための安全な通信を行うための仕組みを導入しています。

①クライアント認証

オンライン届出端末に対し、がん登録オンラインシステムで提供されるクライアント証明書（デジタル証明書）を導入します。クライアント証明書により、システムで許可されたホストに対し、全国がん登録届出サービスへアクセスを提供しています。

②通信経路の暗号化

クライアント型VPNソフトウェアを用いてがん登録オンラインシステムと仮想的なネットワーク(VPN)を確立して通信を行います。このVPNの接続方式では、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」に準拠し、IPsec/IKEによる経路の暗号化を行います。IPsec-VPNを利用することで、通信経路上のデータの機密性を確保し、改ざんや盗聴による被害を防止します。



③IPS/IDSによる不正アクセスの防止

IPS/IDSによりシステムやネットワーク上の不正アクセスに対して、侵入検知・侵入防止を行います。感染型ウイルスに代表される不適切なアクセスからシステムを保護しています。

※IPS/IDSとは、不正遮断／検知システムの略称となります。

⑤ファイルデータの暗号化

届出票（暗号化PDF）は病院・診療所の利用者が独自にパスワードを設定することが可能です。このパスワードは病院・診療所側のみが把握しており、機微な情報に対するデータ秘匿性を担保できます。

④安全なサイトアクセス

医療機関オンライン接続サービスでは、公的認証機関で管理されるSSL証明書で署名されており、サーバの認証／暗号化／改ざん検知を行います。

出典：https://ganjoho.jp/data/reg_stat/cancer_reg/national/hospital/onlinesystem_security.pdf

がん登録オンラインシステムと比較した難病・小慢データベースにおけるセキュリティ対策（案）

難病・小慢 合同委員会
R2. 10. 16 資料1-2 改変

- オンライン化後の難病・小慢DBについては、難病・小慢と同様に、顕名情報を扱うがん登録オンラインシステムと同等以上のセキュリティを確保することとする。
- 通信経路の暗号化については、「医療情報システムの安全管理に関するガイドライン」に準拠した上で、診療所においても接続が行いやすい方式についても検討を行うこととする。
- 指定医の負担軽減等に鑑みれば、指定医以外の医療機関関係者もアクセスできるようにすることが妥当と考えられることから、利用者の操作を監視し、不正な操作がないか監視できるシステムとする。
- 通信経路上を流れるデータについては、自動的に暗号化が図られる仕組みとする。

	①クライアント認証	②通信経路の暗号化	③IPS/IDS※による不正アクセスの防止	④安全なサイトアクセス	⑤ファイルデータの暗号化
がん登録オンラインシステム	クライアント証明書により許可された端末のみ、アクセスを可能とする	IPsec/IKEによる経路を暗号化する	不正アクセスに対して、侵入検知・防止する	公的認証機関で管理されるSSL証明書で署名し、サーバの認証／暗号化／改ざん検知を行う	病院・診療所の利用者が独自にパスワードを設定し暗号化が可能
難病・小慢DB	クライアント証明書により許可された端末のみ、アクセスを可能とする	インターネットVPN (TLS-VPN)による経路を暗号化するとともに、より接続が行いやすい接続方式についても検討	不正アクセスに対して、侵入検知・防止する	公的認証機関で管理されるSSL証明書で署名し、サーバの認証／暗号化／改ざん検知を行う	自動でデータの暗号化を行い、指定医等がアクセスするデータベース上には暗号化して保存する

※ 不正な通信を検知・遮断する仕組み

各医療機関のセキュリティポリシーに則りご確認頂く事項

- 各医療機関で定められているセキュリティポリシーに則り、ご確認頂きたい主な事項を以下に示します。

- ・院内システムからのデータ出力方法
- ・院内ネットワーク上のデータを、外部接続ネットワーク(※)へ移動する方法
※本資料でいうインターネット接続PC端末側のネットワーク
- ・インターネット上で配布するチェックツール(パターン2及び3で利用)の院内ネットワーク環境への持込み方法
 - なお、ツールの配布及び動作環境情報の提供を行いますが、サポート対応までは行わない予定
- ・インターネット環境からの脅威防御対策の実施（新システム利用に関わらず必要な対応）
 - PC端末内のデータの保護と、利用するPC端末が踏み台になることを防止することを想定
 - 例えばファイアウォールの適切な設置、回り込み対策など