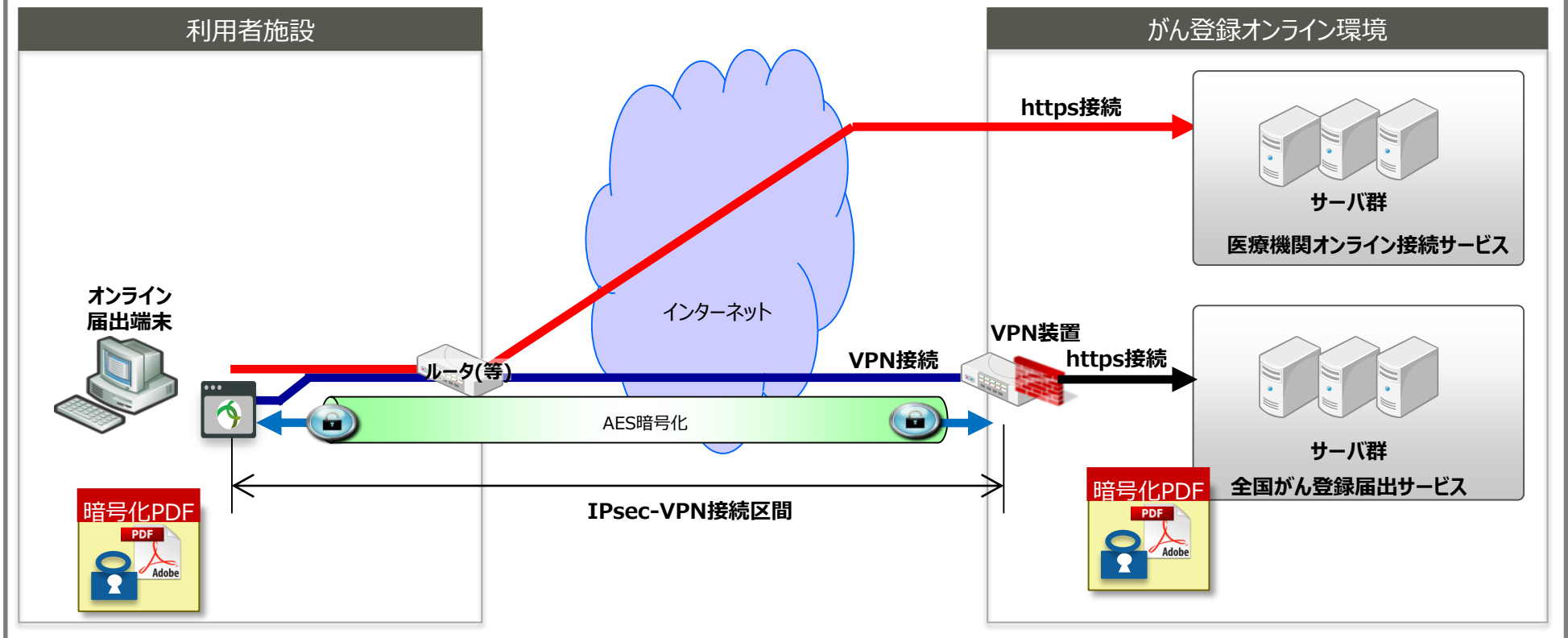


## ■がん登録オンラインシステムの通信概略図

がん登録オンラインシステムは、医療機関オンライン接続サービスへのアクセスを経て、オンライン届出端末とがん登録オンライン環境のVPN接続を行い、利用します。

### 【接続システム概要図】



## ■ 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。

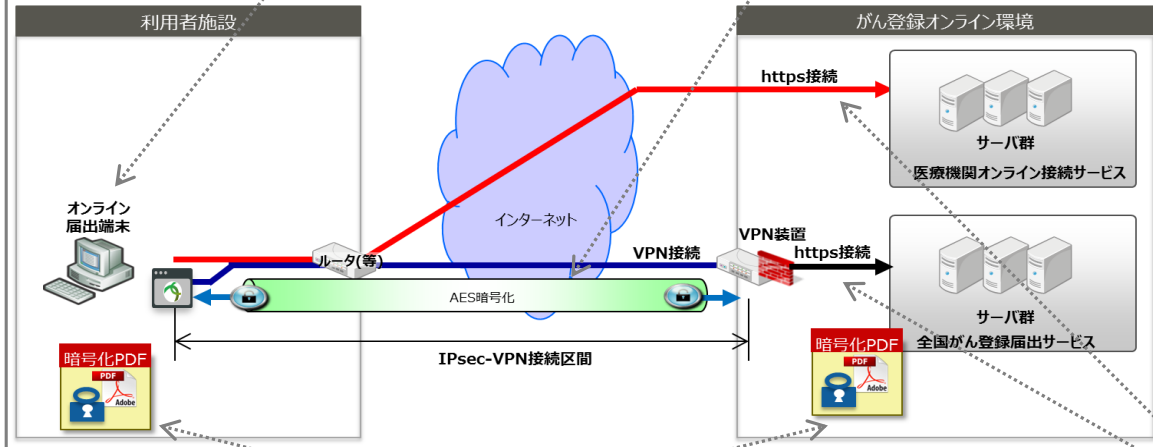
### ①クライアント認証

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。

### 【接続システム概要図】



### 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。

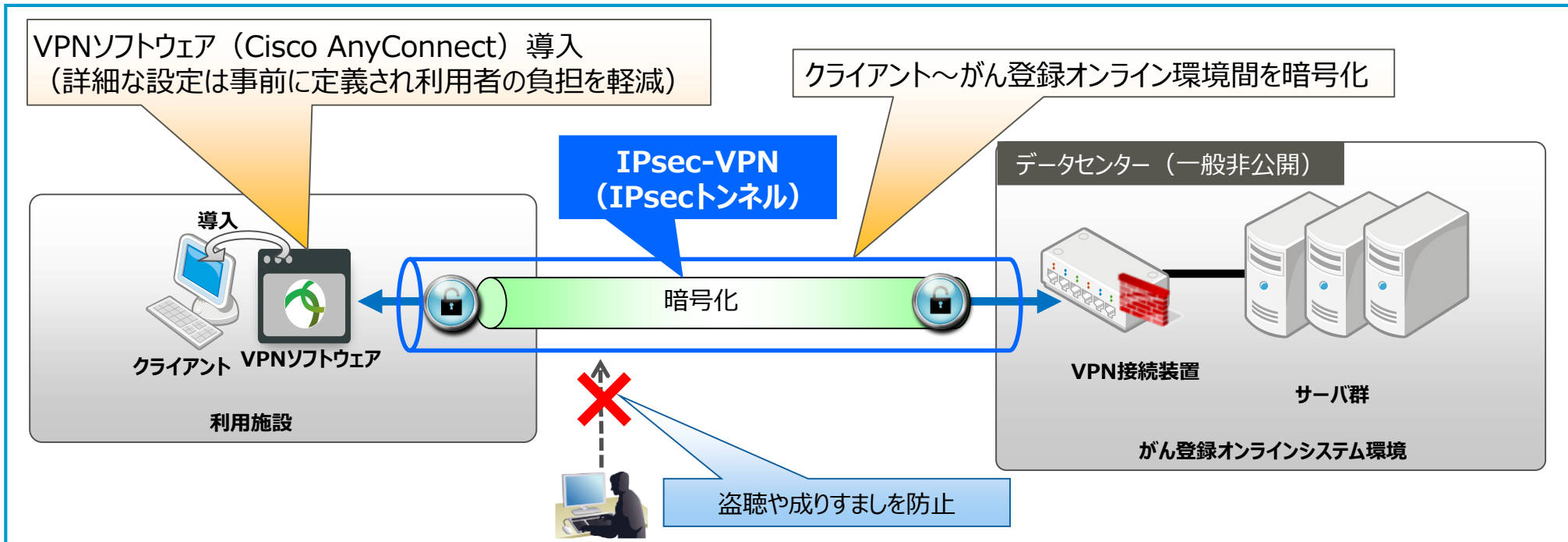
### ④安全なサイトアクセス

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。

## ■がん登録オンラインシステムに用いるIPsec-VPN通信技術について

がん登録オンラインシステムの非公開サイトへアクセスする際は、IPsec-VPNを用いて通信の暗号化を行います。利用施設からがん登録オンラインシステムはインターネットを介した通信を行うため、VPNソフトウェア（Cisco AnyConnect）を導入します。

クライアント型のIPsec-VPNを用いることで安全なIPsecトンネルを確立し、外部からの不正なアクセスを防止します。また、IPsec-VPNのトンネリング機能によりIPパケットの暗号化を行い、パケット内のデータの機密性を確立し、改ざんや盗聴による被害を防止します。



※IPSec・・・Security Architecture for Internet Protocolの略。  
VPN・・・Virtual Private Networkの略。