

医療機関・薬局への導入におけるオンライン資格確認等システムとの接続に係る ネットワーク連携のパターンの参考例

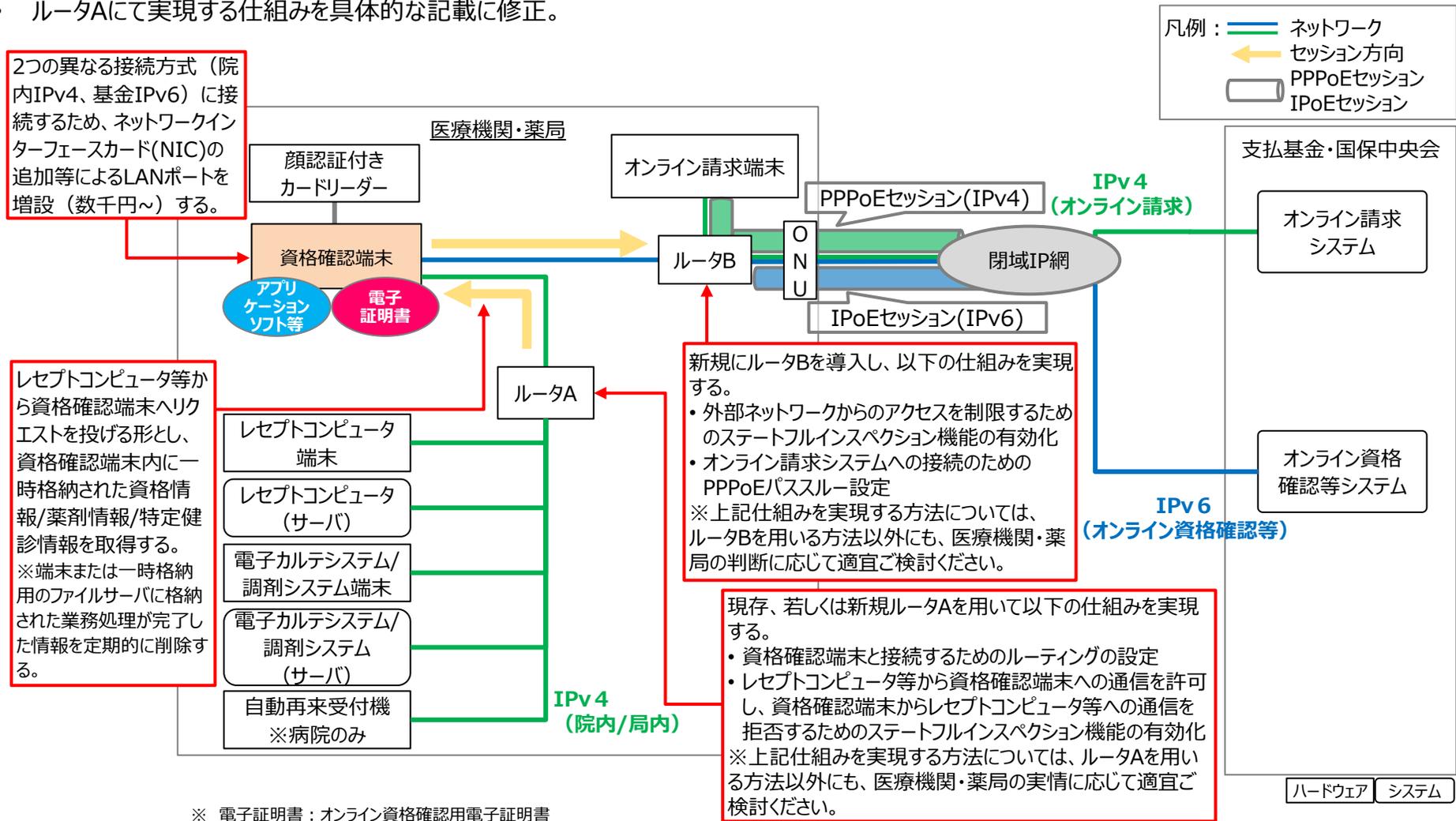
はじめに

- 医療機関等ONS等での問い合わせ傾向を踏まえて、医療機関・薬局への導入におけるオンライン資格確認等システムとの接続に係るネットワーク連携のパターンの参考例の整理を行いました。また、レセプトコンピュータ等の機能を資格確認端末に搭載（もしくはレセプトコンピュータ等端末にアプリケーションソフト等を搭載）する連携パターン例も示します。
- なお、医療機関・薬局への導入に当たっては、連携パターンを参考の上、医療機関・薬局にて「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」に準拠し、必要なセキュリティ対策を行ってください。

○導入後想定：基本的な構成例（資格確認端末が1台もしくは複数台のケース）

【技術解説書1.0版 図2.3.2-2、2-3 基本的な構成例（資格確認端末が1台のケース）（資格確認端末が複数台のケース）からの変更点】

- オンライン請求端末～ONUの間をHUBからルータBに変更。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策をルータBで担うため、記載削除。
- ルータAにて実現する仕組みを具体的な記載に修正。



※ 電子証明書：オンライン資格確認用電子証明書
 ※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる
 ※ IP-VPN回線業者によってはオンライン請求で利用しているPPPoEセッションを利用しIPv4接続方式でオンライン資格確認等システムへ接続する
 ※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

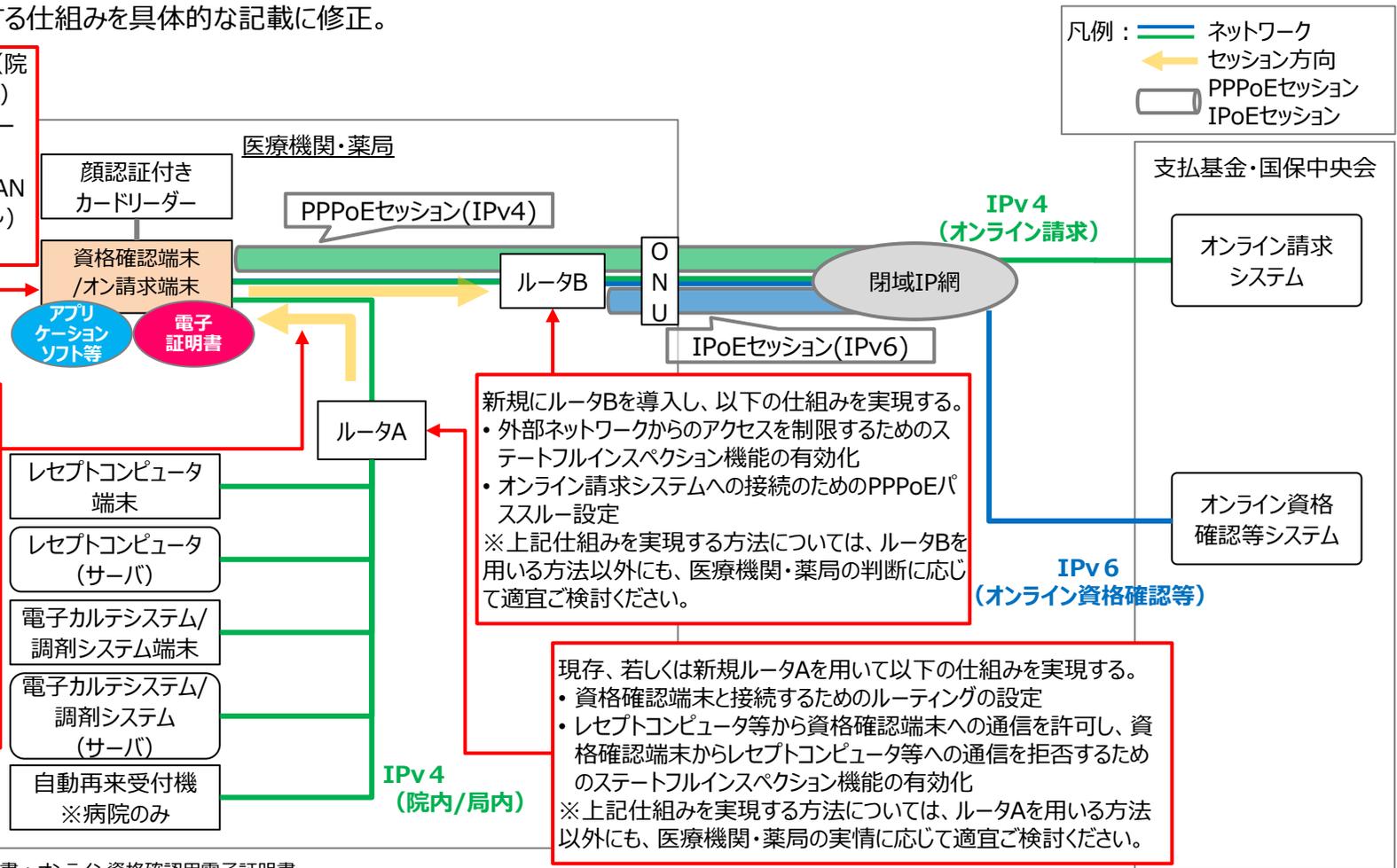
○導入後想定：オンライン請求と資格確認を一台の端末で実施する場合の構成例

【技術解説書1.0版 図2.3.2-4 オンライン請求未対応の施設がオンライン請求と併せて開始する場合の構成例からの変更点】

- オンライン請求端末～ONUの間をHUBからルータBに変更。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策をルータBで担うため、記載削除。
- ルータAにて実現する仕組みを具体的な記載に修正。

2つの異なる接続方式（院内IPv4、基金IPv4/v6）に接続するため、ネットワークインターフェースカード（NIC）の追加等によるLANポートを増設（数千円～）する。

レセプトコンピュータ等から資格確認端末へリクエストを投げる形とし、資格確認端末内に一時格納された資格情報/薬剤情報/特定健診情報を取得する。
※端末または一時格納用のファイルサーバに格納された業務処理が完了した情報を定期的に削除する。



凡例：
— ネットワーク
← セッション方向
 PPPoEセッション
 IPoEセッション

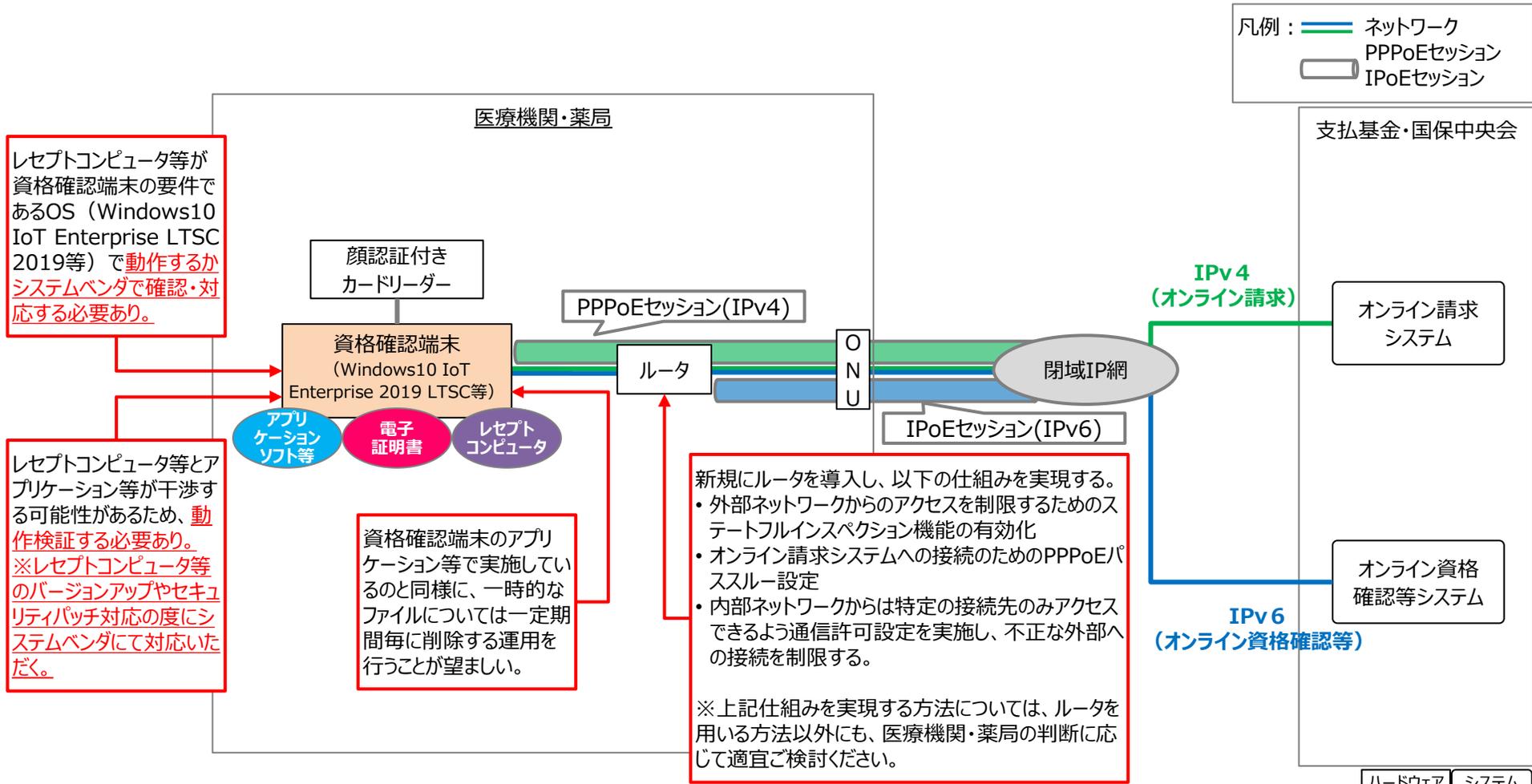
新規にルータBを導入し、以下の仕組みを実現する。
 ・外部ネットワークからのアクセスを制限するためのステートフルインスペクション機能の有効化
 ・オンライン請求システムへの接続のためのPPPoEパススルー設定
 ※上記仕組みを実現する方法については、ルータBを用いる方法以外にも、医療機関・薬局の判断に応じて適宜ご検討ください。

現存、若しくは新規ルータAを用いて以下の仕組みを実現する。
 ・資格確認端末と接続するためのルーティングの設定
 ・レセプトコンピュータ等から資格確認端末への通信を許可し、資格確認端末からレセプトコンピュータ等への通信を拒否するためのステートフルインスペクション機能の有効化
 ※上記仕組みを実現する方法については、ルータAを用いる方法以外にも、医療機関・薬局の実情に応じて適宜ご検討ください。

※ 電子証明書：オンライン資格確認用電子証明書
 ※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる
 ※ IP-VPN回線業者によってはオンライン請求で利用しているPPPoEセッションを利用しIPv4接続方式でオンライン資格確認等システムへ接続する
 ※ IPv6接続方式にて同一端末で「オンライン資格確認等システム」と「オンライン請求システム」を同時利用は、わずかに遅延が発生する可能性があるため、非推奨
 IPv4接続方式の場合は IP-VPN回線業者に確認の上設定する
 ※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会実施できないため、1台のみ接続する

ハードウェア システム

○導入後想定：資格確認端末にレセプトコンピュータ等の機能を搭載する場合の構成例



レセプトコンピュータ等が資格確認端末の要件であるOS (Windows10 IoT Enterprise LTSC 2019等) で動作するかシステムベンダで確認・対応する必要があります。

レセプトコンピュータ等とアプリケーション等が干渉する可能性があるため、動作検証する必要があります。
※レセプトコンピュータ等のバージョンアップやセキュリティパッチ対応の度にシステムベンダにて対応いただく。

資格確認端末のアプリケーション等で実施しているのと同様に、一時的なファイルについては一定期間毎に削除する運用を行うことが望ましい。

新規にルータを導入し、以下の仕組みを実現する。

- 外部ネットワークからのアクセスを制限するためのステートフルインスペクション機能の有効化
- オンライン請求システムへの接続のためのPPPoEパススルー設定
- 内部ネットワークからは特定の接続先のみアクセスできるように通信許可設定を実施し、不正な外部への接続を制限する。

※上記仕組みを実現する方法については、ルータを用いる方法以外にも、医療機関・薬局の判断に応じて適宜ご検討ください。

※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ 資格確認端末の要件であるOSとは、「資格確認端末において満たすべき要件」に示しているOSを指す
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う
 ※ IP-VPN回線業者によってはオンライン請求で利用しているPPPoEセッションを利用しIPv4接続方式でオンライン資格確認等システムへ接続する
 ※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

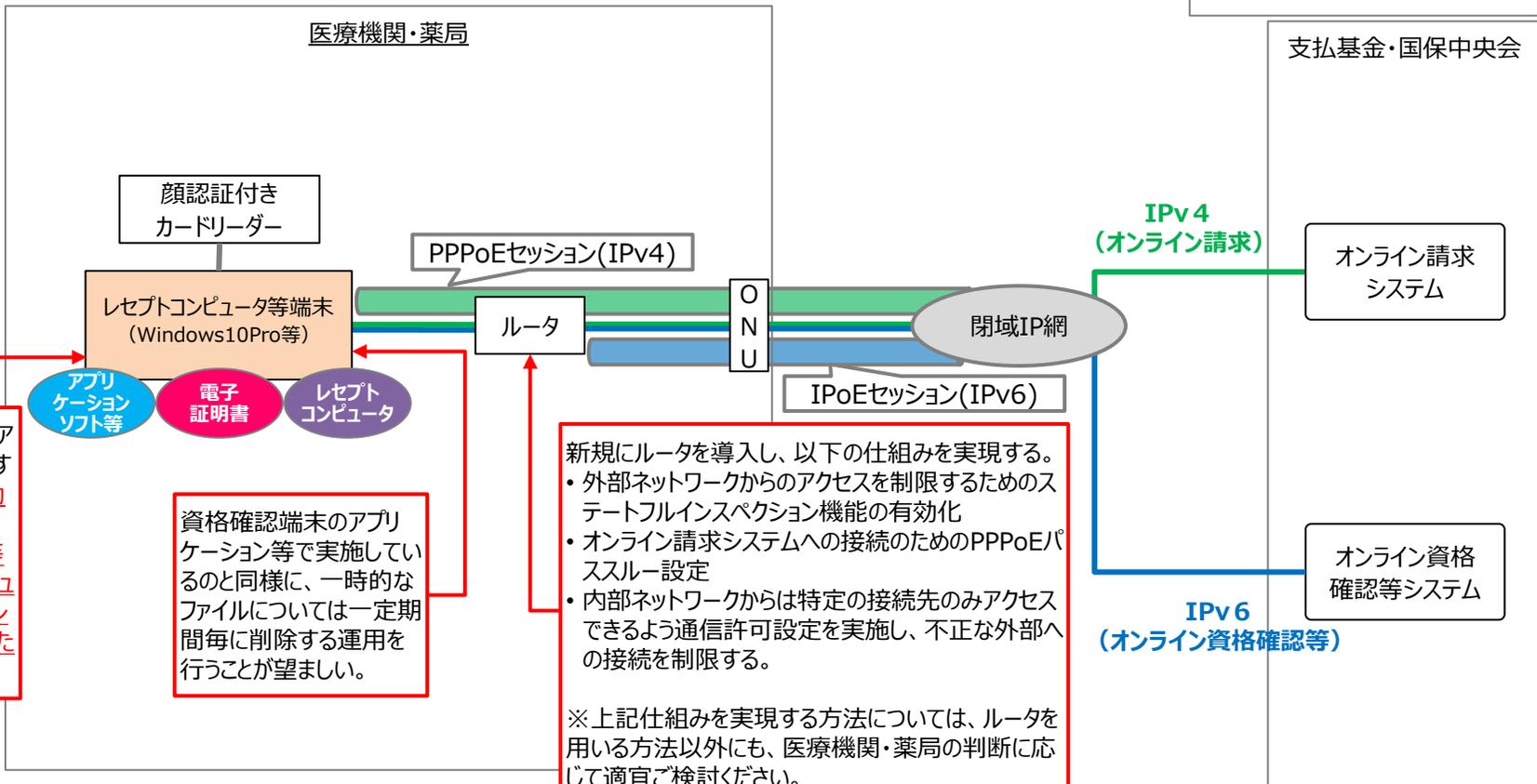
○導入後想定：レセプトコンピュータ等端末に資格確認端末の機能を搭載する場合の構成例

資格確認端末において満たすべき要件以外のマイナンバーカード処理ソフト・オンライン資格確認等連携ソフトが動作する対象OS

- Windows10Pro
- Windows10 Enterprise SAC
- Windows10 IoT Enterprise SAC

<補足>
 サポート対象OSについて、OSにおけるサポートライフサイクルやサポート期間、医療機関・薬局での利用状況を踏まえて、Windows OSを選定している。
 (令和2年8月時点)

凡例：
 ネットワーク
 PPPoEセッション
 IPoEセッション



レセプトコンピュータ等とアプリケーション等が干渉する可能性があるため、**動作検証する必要あり。**
 ※レセプトコンピュータ等のバージョンアップやセキュリティパッチ対応の度にシステムベンダにて対応いただく。

資格確認端末のアプリケーション等で実施しているのと同様に、一時的なファイルについては一定期間毎に削除する運用を行うことが望ましい。

新規にルータを導入し、以下の仕組みを実現する。

- 外部ネットワークからのアクセスを制限するためのステートフルインスペクション機能の有効化
- オンライン請求システムへの接続のためのPPPoEパススルー設定
- 内部ネットワークからは特定の接続先のみアクセスできるように通信許可設定を実施し、不正な外部への接続を制限する。

※上記仕組みを実現する方法については、ルータを用いる方法以外にも、医療機関・薬局の判断に応じて適宜ご検討ください。

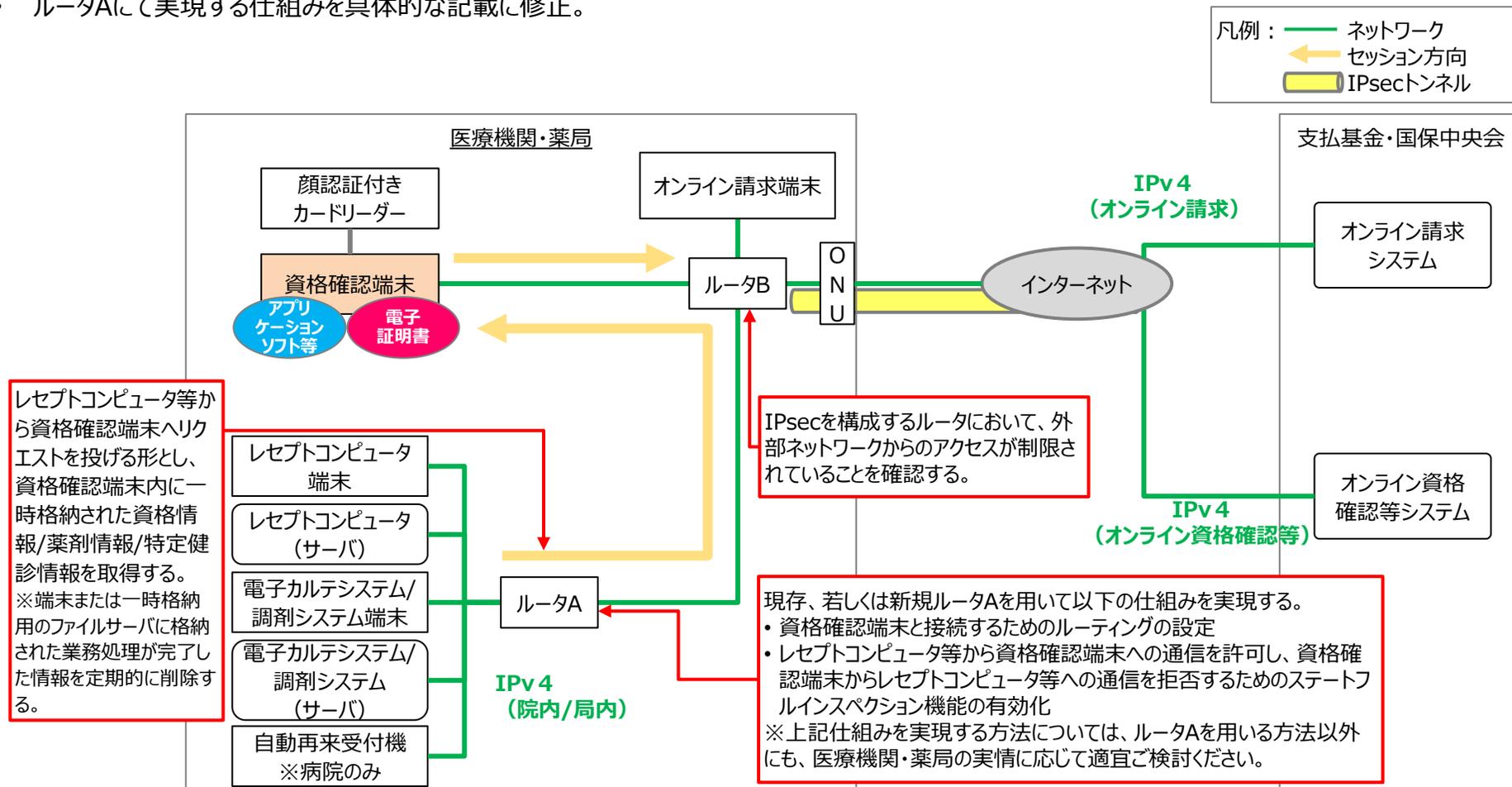
※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う
 ※ IP-VPN回線業者によってはオンライン請求で利用しているPPPoEセッションを利用しIPv4接続方式でオンライン資格確認等システムへ接続する

ハードウェア システム

○導入後想定：基本的な構成例（資格確認端末が1台もしくは複数台のケース）

【技術解説書1.0版 図2.3.2-6、2-7 基本的な構成例（資格確認端末が1台のケース）（資格確認端末が複数台のケース）からの変更点】

- ルータ型であるため、オンライン請求端末～ONUの間をHUBからルータBに変更。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策を現存するルータBで担うため、記載削除。
- 資格確認端末での通信接続方式がIPv4のみであり、通信経路の物理的対策は不要となったため、ネットワークインターフェースカードの追加を削除。
- ルータAにて実現する仕組みを具体的な記載に修正。



※ 電子証明書：オンライン資格確認用電子証明書

※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる

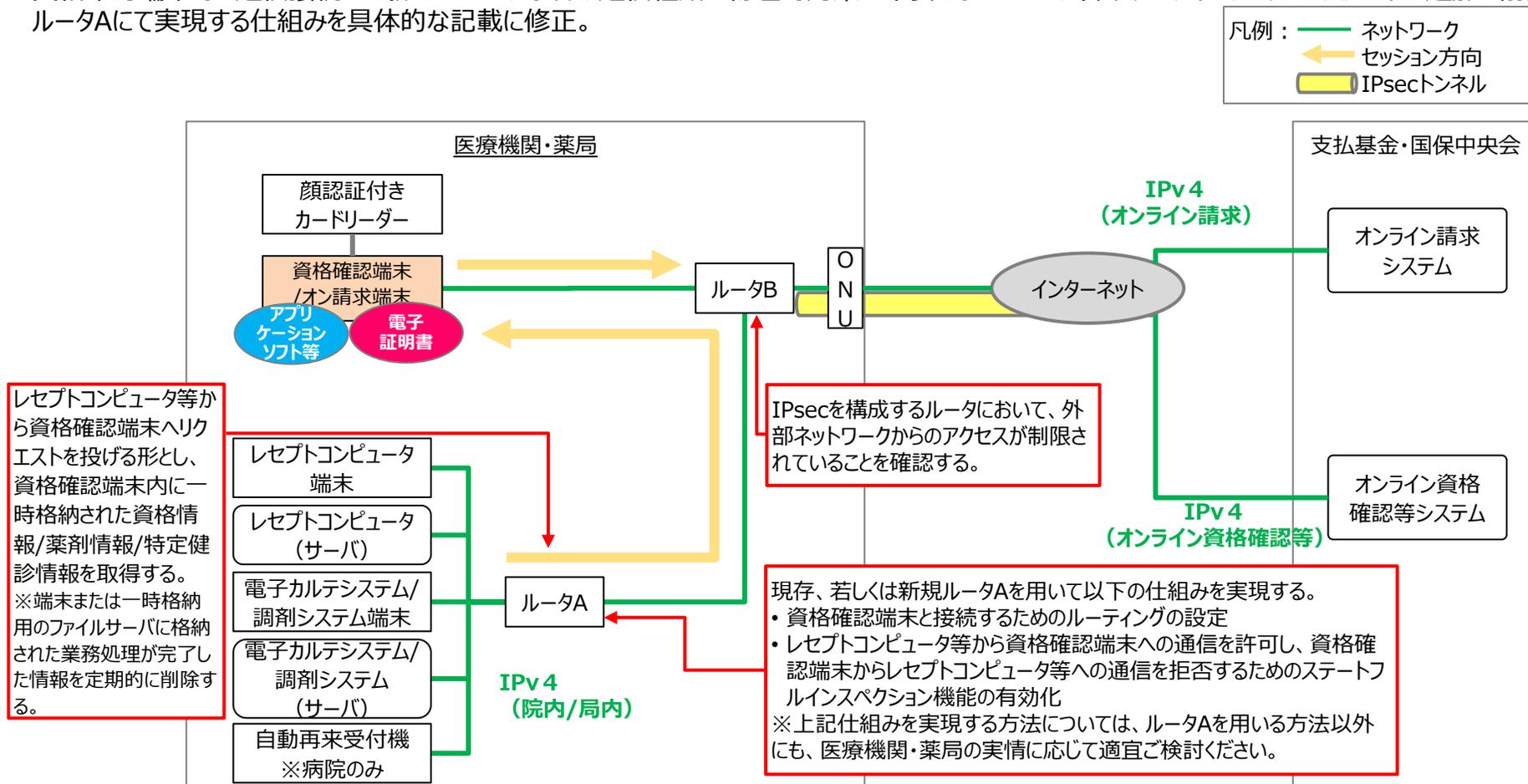
※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

ハードウェア システム

○導入後想定：オンライン請求未対応の施設がオンライン請求と併せて開始する場合の構成例

【技術解説書1.0版 図2.3.2-8 オンライン請求未対応の施設がオンライン請求と併せて開始する場合の構成例からの変更点】

- ルータ型であるため、オンライン請求端末～ONUの間をHUBからルータBに変更。
- 上記に伴い、ルータにて通信経路を振り分けるため、LANポート差し抜き運用の記載を削除。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策を現存するルータBで担うため、記載削除。
- 資格確認端末での通信接続方式がIPv4のみであり、通信経路の物理的対策は不要となったため、ネットワークインターフェースカードの追加を削除。
- ルータAにて実現する仕組みを具体的な記載に修正。



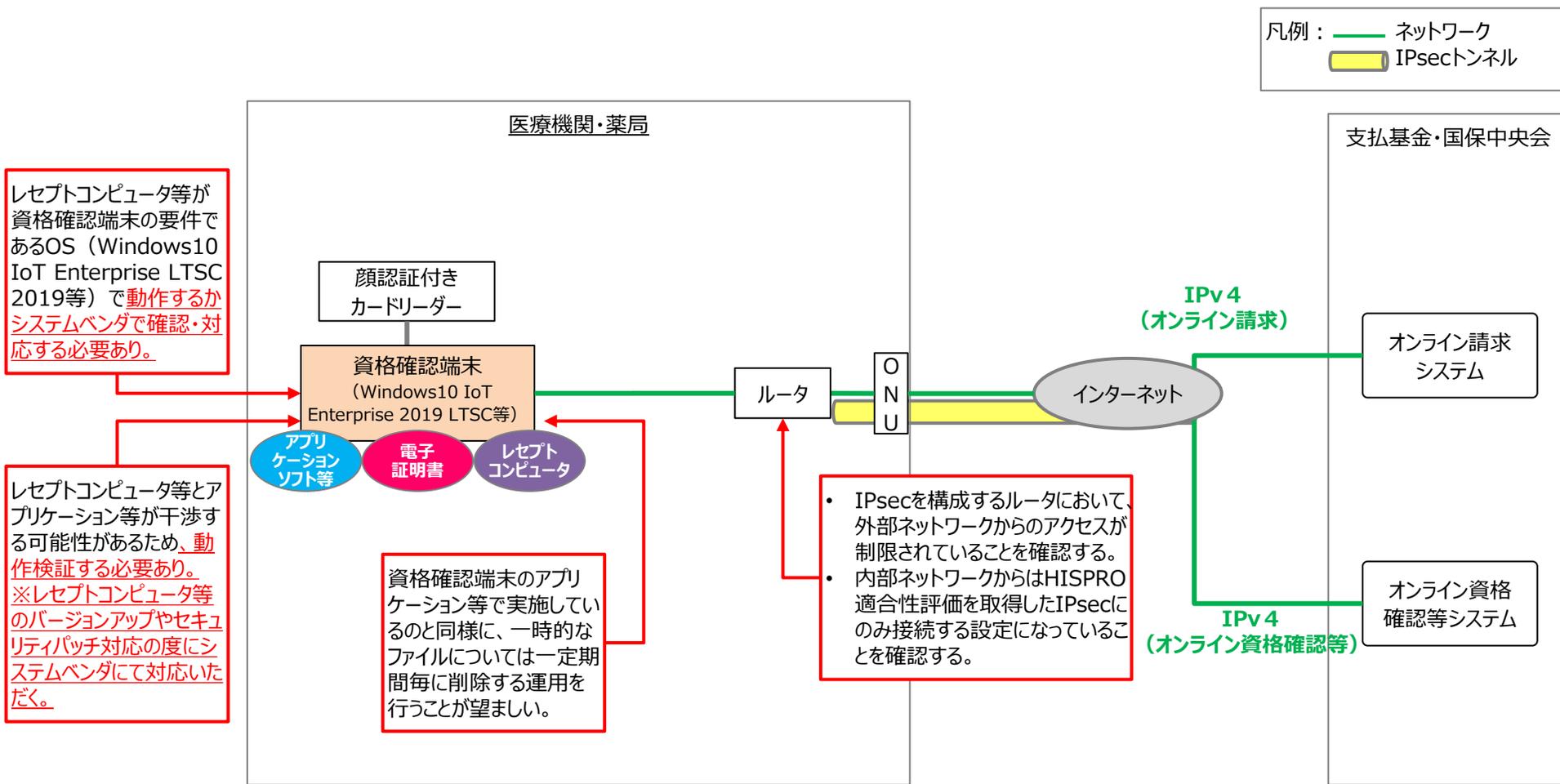
※ 電子証明書：オンライン資格確認用電子証明書

※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる

※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

ハードウェア システム

○導入後想定：資格確認端末にレセプトコンピュータ等端末の機能を搭載する場合の構成例



※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ 資格確認端末の要件であるOSとは、「資格確認端末において満たすべき要件」に示しているOSを指す
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う
 ※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

○導入後想定：レセプトコンピュータ等端末に資格確認端末の機能を搭載する場合の構成例

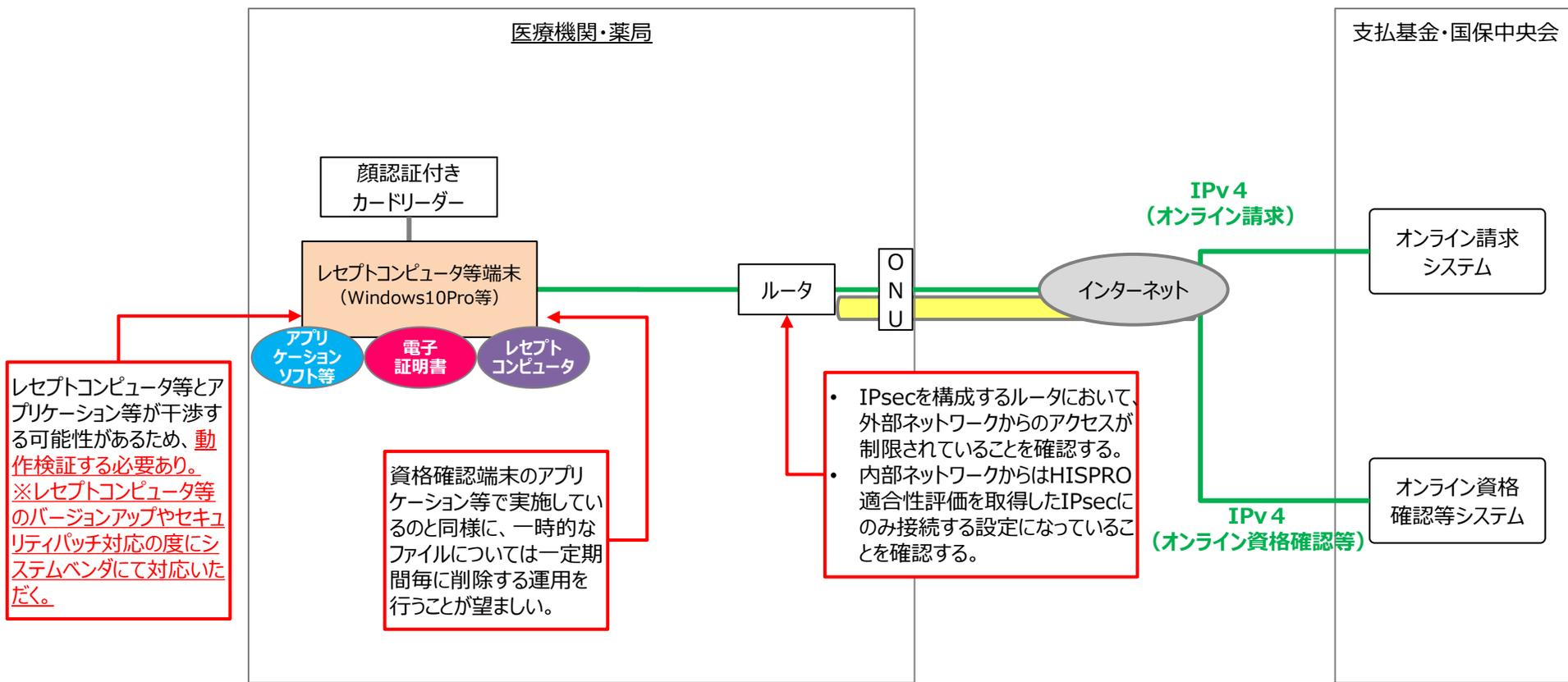
資格確認端末において満たすべき要件以外のマイナンバーカード処理ソフト・オンライン資格確認等連携ソフトが動作する対象OS

- Windows10Pro
- Windows10 Enterprise SAC
- Windows10 IoT Enterprise SAC

<補足>

サポート対象OSについて、OSにおけるサポートライフサイクルやサポート期間、医療機関・薬局での利用状況を踏まえて、Windows OSを選定している。
(令和2年8月時点)

凡例： — ネットワーク
 IPsecトンネル



レセプトコンピュータ等とアプリケーション等が干渉する可能性があるため、動作検証する必要あり。
 ※レセプトコンピュータ等のバージョンアップやセキュリティパッチ対応の度にシステムベンダにて対応いただく。

資格確認端末のアプリケーション等を実施しているのと同様に、一時的なファイルについては一定期間毎に削除する運用を行うことが望ましい。

- IPsecを構成するルータにおいて、外部ネットワークからのアクセスが制限されていることを確認する。
- 内部ネットワークからはHISPRO適合性評価を取得したIPsecにのみ接続する設定になっていることを確認する。

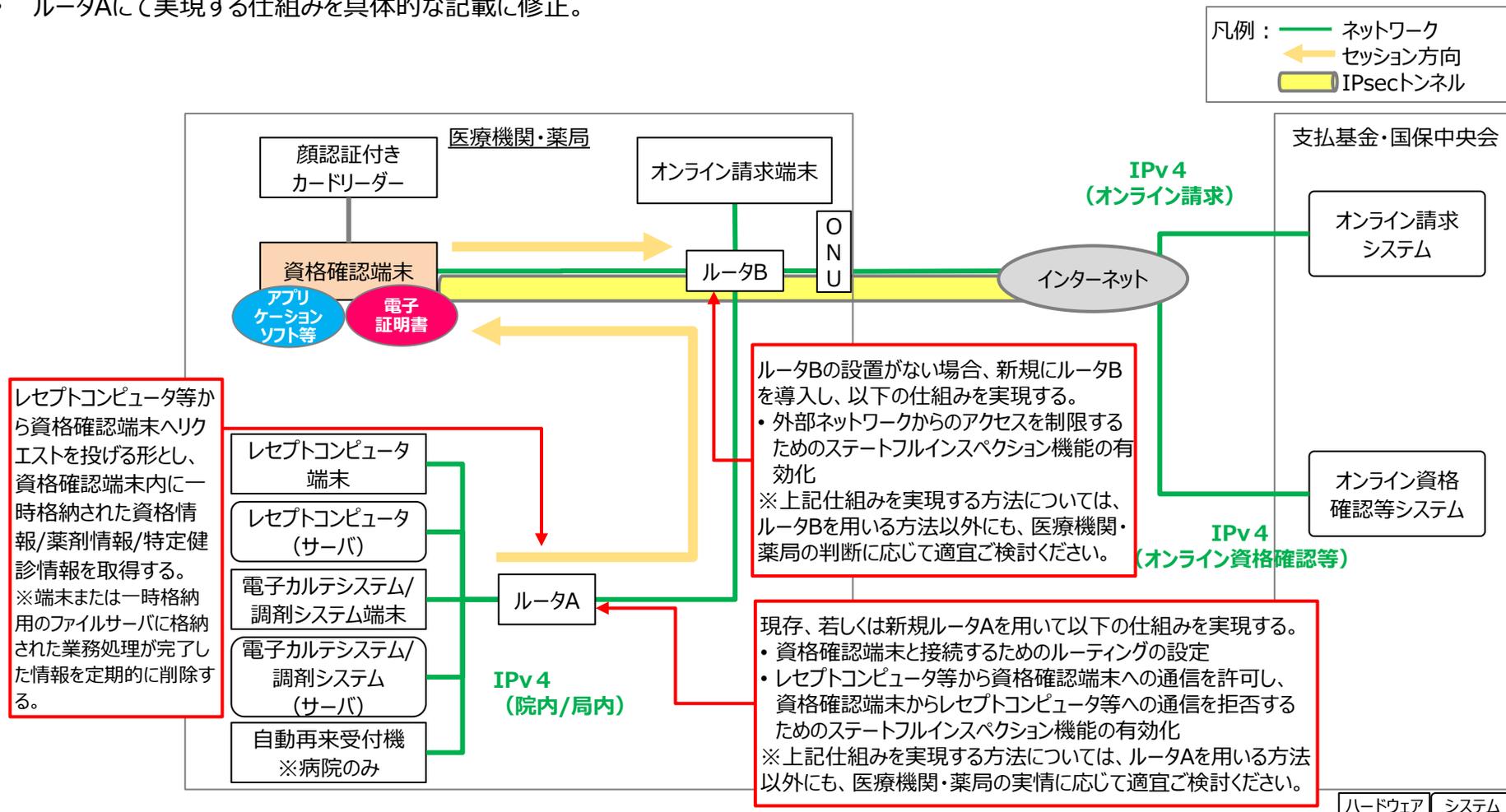
※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う

ハードウェア システム

○導入後想定：基本的な構成例（資格確認端末が1台もしくは複数台のケース）

【技術解説書1.0版 図2.3.2-6、2-7 基本的な構成例（資格確認端末が1台のケース）（資格確認端末が複数台のケース）からの変更点】

- ルータ型であるため、オンライン請求端末～ONUの間をHUBからルータBに変更し、実現する仕組みを具体的に記載。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策を現存するルータBで担うため、記載削除。
- 資格確認端末での通信接続方式がIPv4のみであり、通信経路の物理的対策は不要となったため、ネットワークインターフェースカードの追加を削除。
- ルータAにて実現する仕組みを具体的な記載に修正。



※ 電子証明書：オンライン資格確認用電子証明書

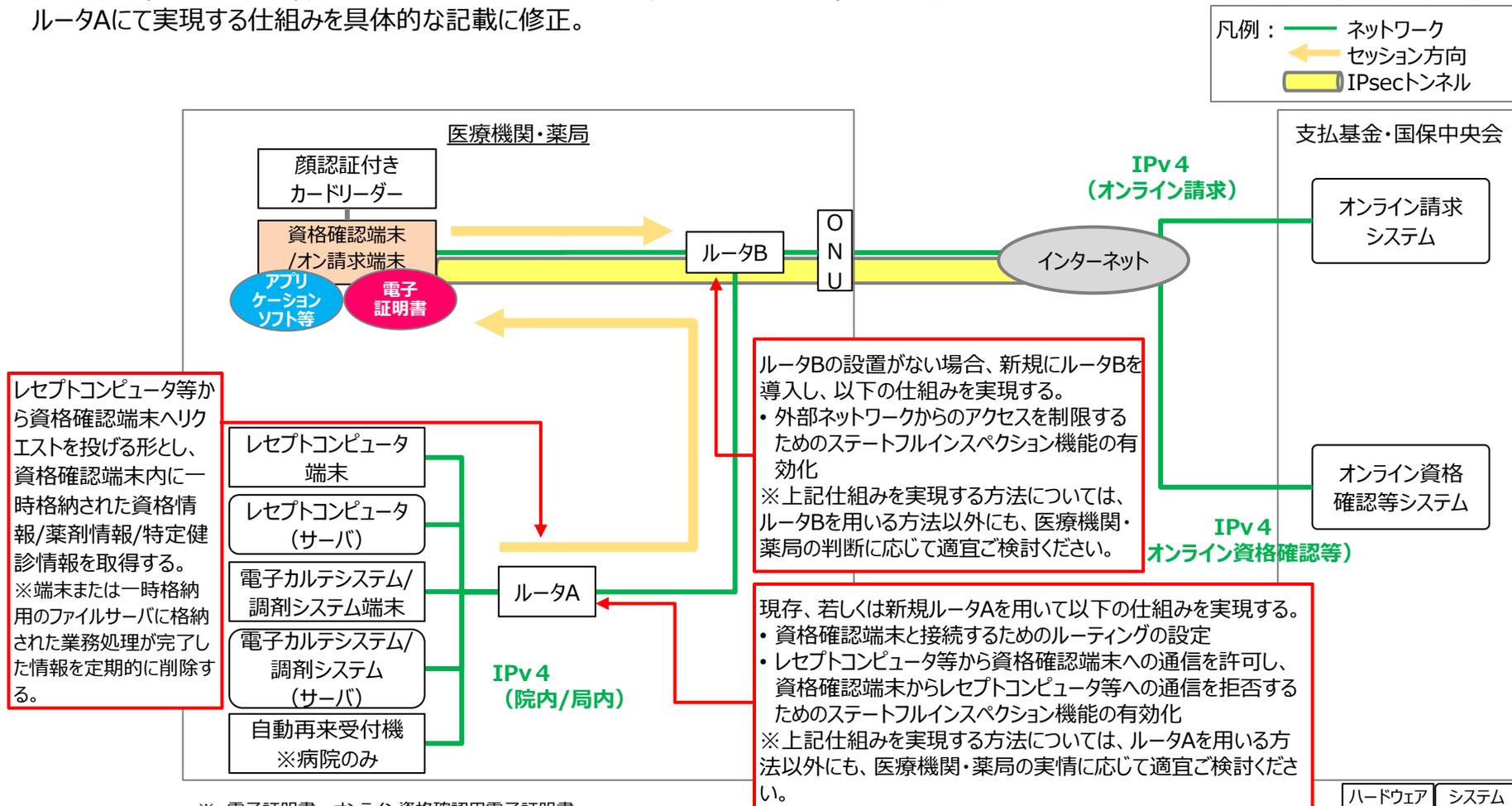
※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる

※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会の実施できないため、1台のみ接続する

○導入後想定：オンライン請求未対応の施設がオンライン請求と併せて開始する場合の構成例

【技術解説書1.0版 図2.3.2-8 オンライン請求未対応の施設がオンライン請求と併せて開始する場合の構成例からの変更点】

- ルータ型であるため、オンライン請求端末～ONUの間をHUBからルータBに変更し、実現する仕組みを具体的に記載。
- 上記に伴い、ルータにて通信経路を振り分けるため、LANポート差し抜き運用の記載を削除。
- 資格確認端末内のソフトウェアファイアウォールによる外部ネットワークアクセス制御の対策を現存するルータBで担うため、記載削除。
- 資格確認端末での通信接続方式がIPv4のみであり、通信経路の物理的対策は不要となったため、ネットワークインターフェースカードの追加を削除。
- ルータAにて実現する仕組みを具体的な記載に修正。



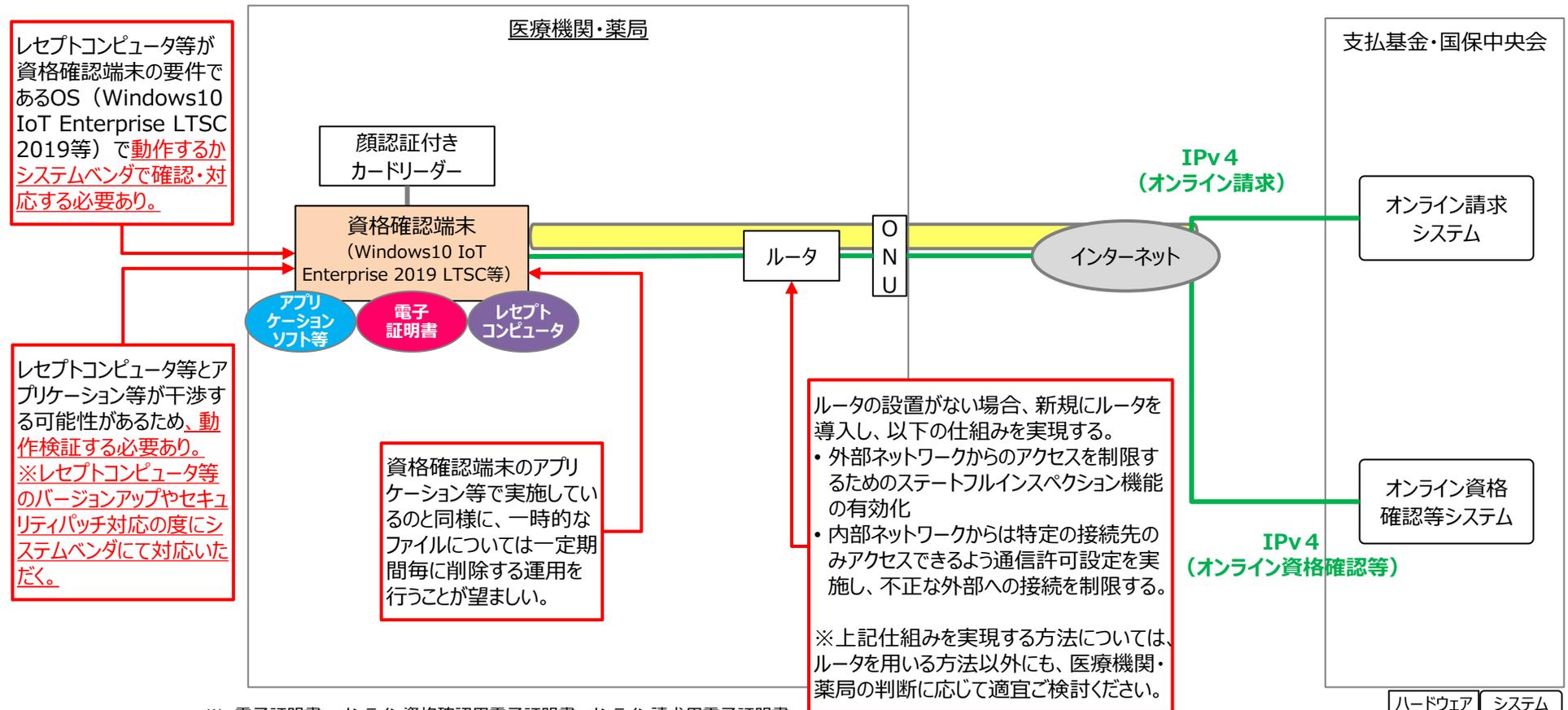
※ 電子証明書：オンライン資格確認用電子証明書

※ 「セッション方向」とは、起点からの方向を指しているものであり、情報のやり取りは双方向で行われる

※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会には実施できないため、1台のみ接続する

○導入後想定：資格確認端末にレセプトコンピュータ等端末の機能を搭載する場合の構成例

凡例： — ネットワーク
 IPsecトンネル



レセプトコンピュータ等が
資格確認端末の要件で
あるOS (Windows10
IoT Enterprise LTSC
2019等) で動作するか
システムベンダで確認・対
応する必要があります。

レセプトコンピュータ等とア
プリケーション等が干渉す
る可能性があるため、動
作検証する必要があります。
※レセプトコンピュータ等
のバージョンアップやセキュ
リティパッチ対応の度にシ
ステムベンダにて対応いた
だく。

資格確認端末のアプリ
ケーション等で実施してい
ると同様に、一時的な
ファイルについては一定期
間毎に削除する運用を
行うことが望ましい。

ルータの設置がない場合、新規にルータを
導入し、以下の仕組みを実現する。

- 外部ネットワークからのアクセスを制限するためのステートフルインスペクション機能の有効化
- 内部ネットワークからは特定の接続先のみアクセスできるよう通信許可設定を実施し、不正な外部への接続を制限する。

※上記仕組みを実現する方法については、
ルータを用いる方法以外にも、医療機関・
薬局の判断に応じて適宜ご検討ください。

※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ 資格確認端末の要件であるOSとは、「資格確認端末において満たすべき要件」に示しているOSを指す
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う
 ※ 資格確認端末に顔認証付きカードリーダーおよび汎用カードリーダーの両方を接続している場合マイナンバーカードによる資格情報照会とは実施できないため、1台のみ接続する

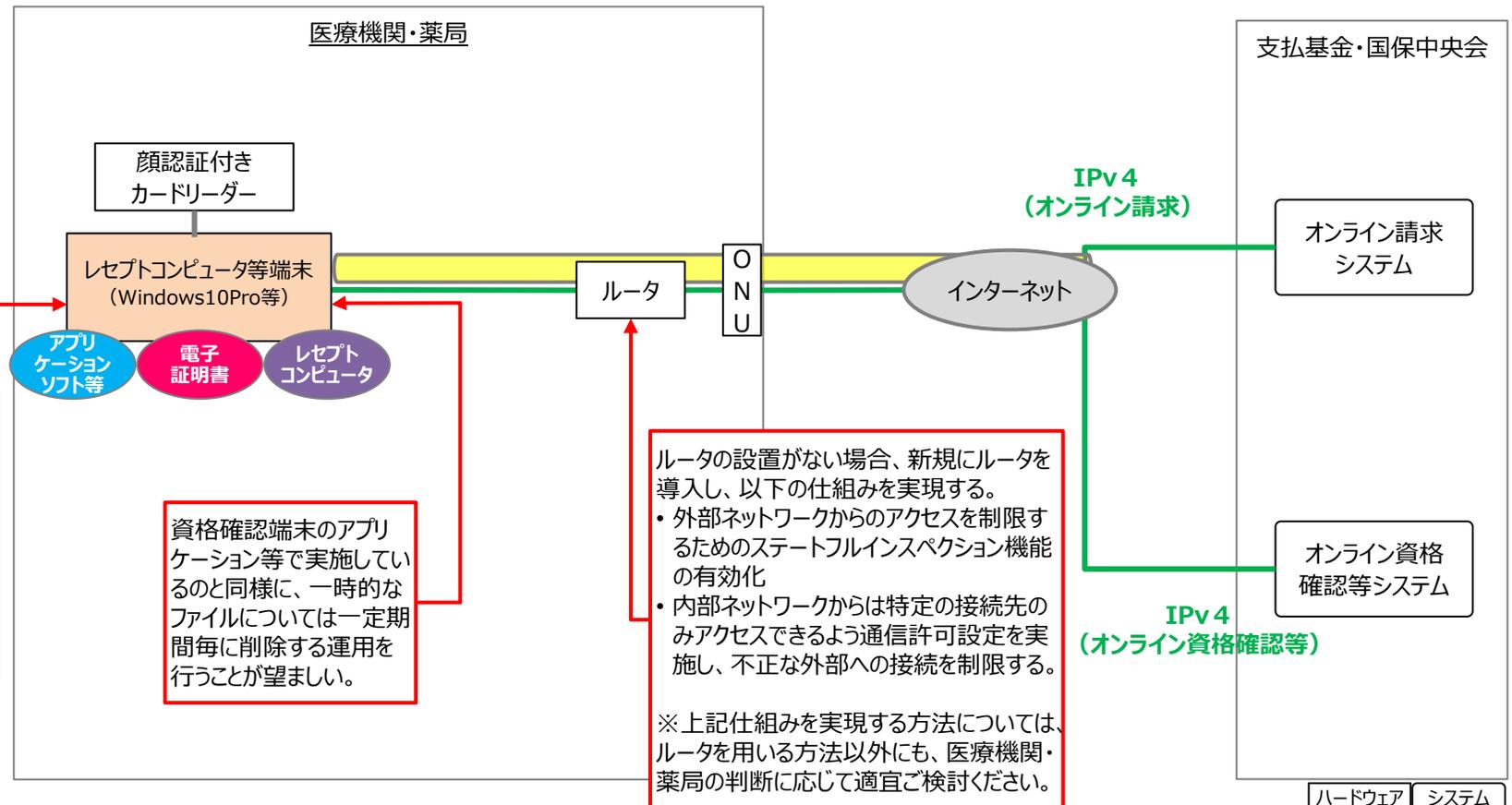
○導入後想定：レセプトコンピュータ等端末に資格確認端末の機能を搭載する場合の構成例

資格確認端末において満たすべき要件以外のマイナンバーカード処理ソフト・オンライン資格確認等連携ソフトが動作する対象OS

- Windows10Pro
- Windows10 Enterprise SAC
- Windows10 IoT Enterprise SAC

<補足>
サポート対象OSについて、OSにおけるサポートライフサイクルやサポート期間、医療機関・薬局での利用状況を踏まえて、Windows OSを選定している。
(令和2年8月時点)

凡例： — ネットワーク
 IPsecトンネル



レセプトコンピュータ等とアプリケーション等が干渉する可能性があるため、動作検証する必要あり。
※レセプトコンピュータ等のバージョンアップやセキュリティパッチ対応の度にシステムベンダにて対応いただく。

資格確認端末のアプリケーション等で実施しているのと同様に、一時的なファイルについては一定期間毎に削除する運用を行うことが望ましい。

ルータの設置がない場合、新規にルータを導入し、以下の仕組みを実現する。

- 外部ネットワークからのアクセスを制限するためのステートフルインスペクション機能の有効化
- 内部ネットワークからは特定の接続先のみアクセスできるよう通信許可設定を実施し、不正な外部への接続を制限する。

※上記仕組みを実現する方法については、ルータを用いる方法以外にも、医療機関・薬局の判断に応じて適宜ご検討ください。

※ 電子証明書：オンライン資格確認用電子証明書、オンライン請求用電子証明書
 ※ レセプトコンピュータの構成によって、サーバ等を設置する構成もあり
 ※ レセプトコンピュータの構成としてサーバ等を設置している場合、ルータから分岐して接続されるサーバやルータにてアクセス制限対策を行う