参考資料３-９

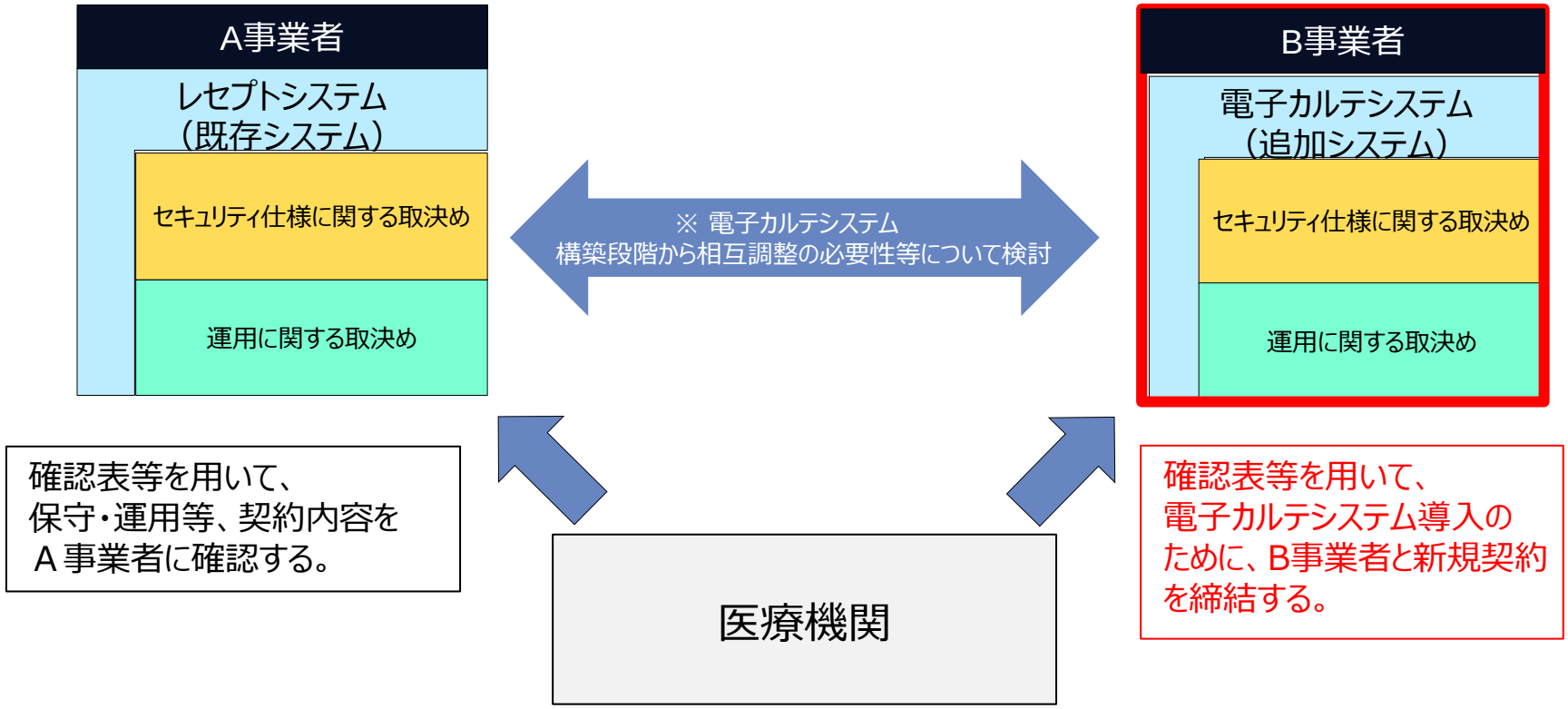
別添３

新規システムの導入に際しての「医療情報システムの契約における当事者間の役割分担等に関する確認表」の利用イメージ

（例）既にレセプトシステム（A事業者）を導入しており、新たに電子カルテシステムを導入するためにB事業者と契約を締結する場合

- 医療機関は、確認表等を用いて、保守・運用等、既存の契約内容をＡ事業者に確認する。
- 加えて、電子カルテシステムの導入に際して、確認表等を用いて、B事業者との契約内容を確認する。

※ 事業者間の役割及び抜け漏れがないように、電子カルテシステム構築段階から事業者間で相互調整等を行う。
B事業者は、医療機関との新規契約の中で、A事業者との相互調整の必要性等について検討を行う。
A事業者は、医療機関との既存契約の中で、B事業者との相互調整の必要性等について検討を行う。



医療機関のセキュリティ対応上の課題（各課題に対する本確認表の利用イメージの例等は、次ページ以降参照）

- 医療機関のセキュリティ対応上の課題として、以下の4つを整理した。
- 医療機関と事業者が協力しながら、本確認表を活用すること等を通じて、こうした課題に対応する必要がある。

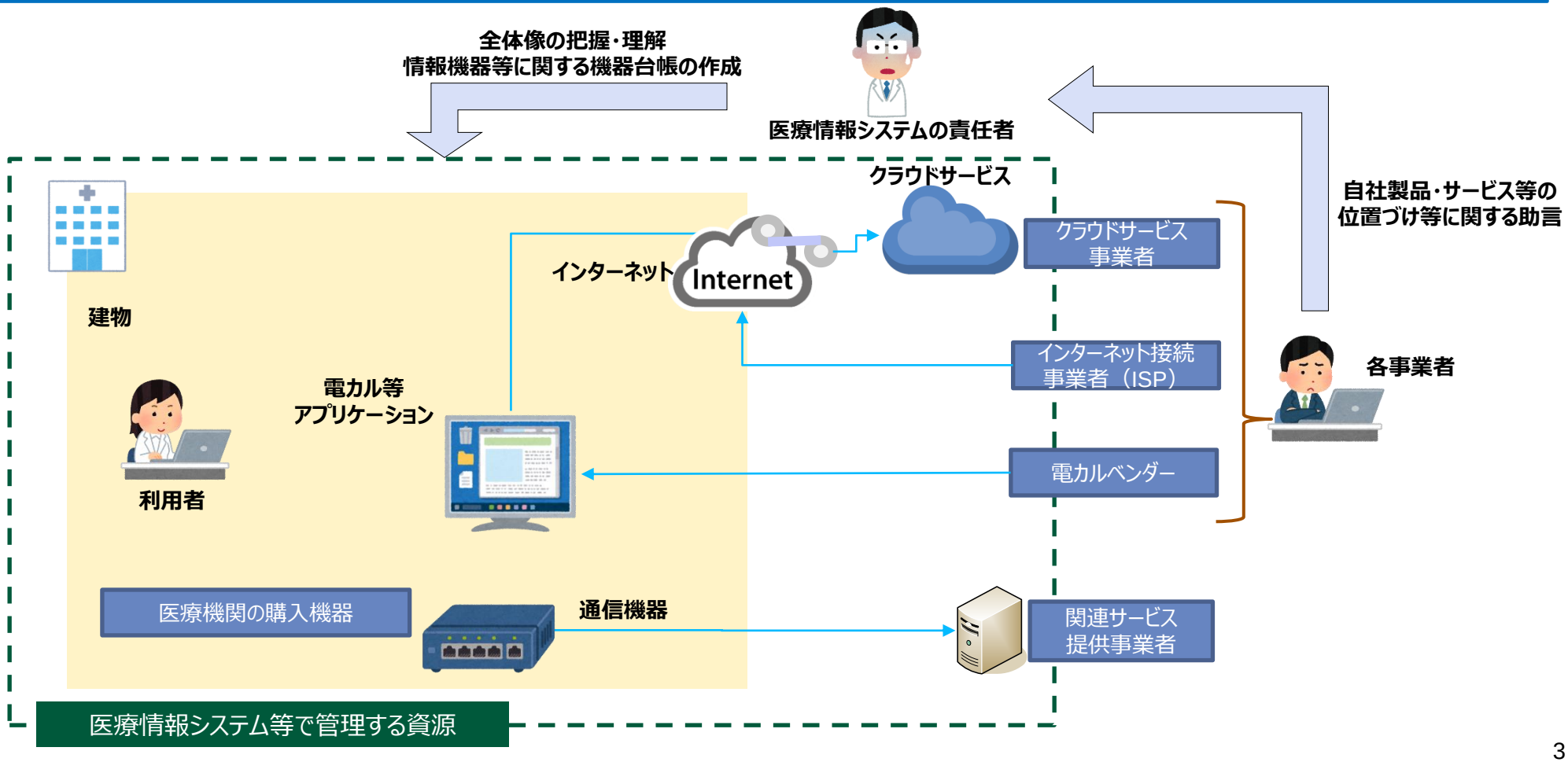
医療機関のセキュリティ対応上の課題		医療機関側の要因	医療機関と事業者で可能な対応	対応する本確認表の項目例
①	医療機関が保有する資源を網羅的に把握できていない	• 利用している医療情報システムの全体像が理解されていない • 医療機関以外には、全体像を利用できる者がいない • 機器等は買い切りの場合には、医療機関が自ら情報管理する必要がある	• 医療機関は、事業者から、医療機関が管理するシステム構成図に対して、自社製品・サービス等の位置づけ等に関する助言の提供を受けた上で、医療機関と事業者双方で協力して対応する	• 情報機器等（サーバ、端末PC、ネットワーク機器等）の台帳管理 【推奨される対応例 Part1 参考3①】
②	医療機関が管理する資源に係る最新の脆弱性情報等が把握できていない	• 医療機関において脆弱性に関する情報を管理する知見等がない • 医療機関において、情報収集のためのスキームを構築していない	• 医療機関は、事業者から、契約等に基づく情報や事業者における最新情報の提供を受けた上で、医療機関と事業者双方で協力して対応する	• 脆弱性情報の確認・報告【推奨される対応例 Part2 参考1】 • ＯＳやアプリケーション、ハードウェアの保守の実施 【推奨される対応例 Part2 参考6】
③	医療機関が管理する資源に対する理解が不足している	• 医療機関にリスクに関する情報を理解し対応できる知見を有する人材がいない • 対応できないことに対して、適切な対応がなされていない	• 医療機関は、事業者から、医療機関が管理する資源について、医療機関の理解が促されるような形での情報提供を受けた上で、医療機関と事業者双方で協力して対応する	• 医療情報を取り扱う職員に対する人的安全管理対策の実施【Part1 B3①】 • 個人情報の安全管理に関する職員への教育・訓練の実施及び実施状況に係る報告【Part1 B3②】 • 医療情報システムのセキュリティに関する情報提供義務【Part2 A11】
④	医療機関が管理する資源において、一部の資源に対する脆弱性対策が、他の資源の可用性に影響を与える可能性がある場合に、安全性の判断ができない	• 医療機関が優先すべき資源を判断し、リスクへの対応を行う必要があるが、できていない	• 医療機関は、事業者から、システム、機器等の脆弱性対策の組合せによる可用性への影響に関する情報等の共有や代替的なリスク低減・回避方策の提案を受けた上で、医療機関と事業者双方で協力して対応する	• 脆弱性情報の確認・報告【推奨される対応例 Part2 参考1】＜再掲＞ • ＯＳやアプリケーション、ハードウェアの保守の実施 【推奨される対応例 Part2 参考6】＜再掲＞ • セキュリティ対策の見直し提案【Part2 A12】

※「資源」とは、医療情報システムを構成する情報機器、ソフトウェア、インフラ等のこと。

課題①：医療機関が保有する資源を網羅的に把握できていない

■ 情報機器等（サーバ、端末PC、ネットワーク機器等）の台帳管理【推奨される対応例 Part1 参考3①】

(a) 情報機器等（※）の所在と、それらの使用可否の状態を適切に管理するため、機器台帳を作成して、情報機器等の所在や利用者、ソフトウェアやサービスのバージョン等の管理を行い、情報機器等が利用に適した状況にあることを確認できるようにする。事業継続の観点から紙及びクラウド等を用いた管理等、台帳管理を行う媒体の種類及び媒体数等も検討すること。
（※）サーバ、端末PC、ネットワーク機器のほか、ネットワークに接続される可能性がある医療機器等も含む。
(b) 必要に応じて事業者と協力しながら、リモートメンテナンス（保守）を利用している機器の有無の把握も行う。



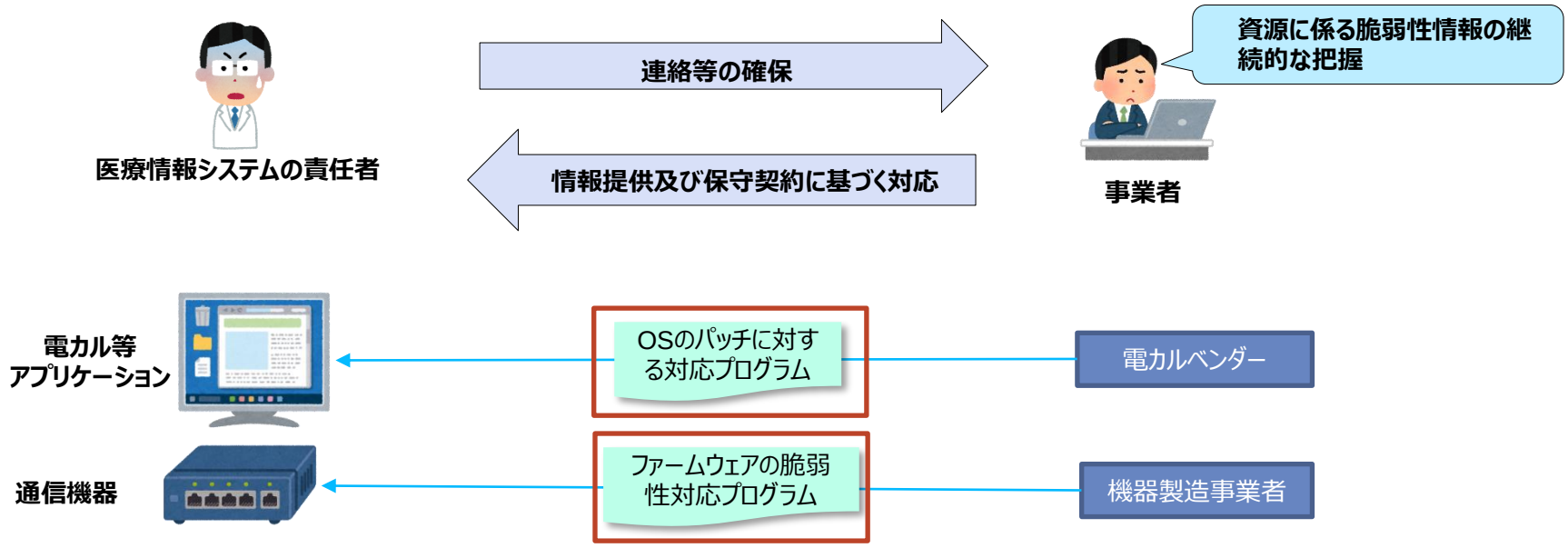
課題②：医療機関が管理する資源に係る最新の脆弱性情報等が把握できていない

■ 脆弱性情報の確認・報告 【推奨される対応例 Part2 参考1】

医療情報システムに関連する新たなセキュリティ上の脆弱性について、(独) 情報処理推進機構（IPA）等が公表する情報その他の情報を継続的に収集すること（又は合理的な範囲で収集に努めること）、および脆弱性発見時の医療機関への報告や対策の実施を行うこと等を取り決める。

■ ＯＳやアプリケーション、ハードウェアの保守の実施 【推奨される対応例 Part2 参考6】

システムを構成する機器、ソフトウェア、クラウドサービス等については、保守契約に基づき事業者による保守（セキュリティパッチの適用等）がなされるよう取り決める。オープンソースソフトウェア等の汎用ソフトウェアを使用する際も、脆弱性情報等のチェックやその対応についても取り決める。



課題③：医療機関が管理する資源に対する理解が不足している

■ 医療情報を取り扱う職員に対する人的安全管理対策の実施 【Part1 B3①】

医療情報を取り扱う職員に対し、退職後を含めた守秘義務や教育・訓練等を受ける義務を課す雇用契約等を締結することで、人的管理を行う。

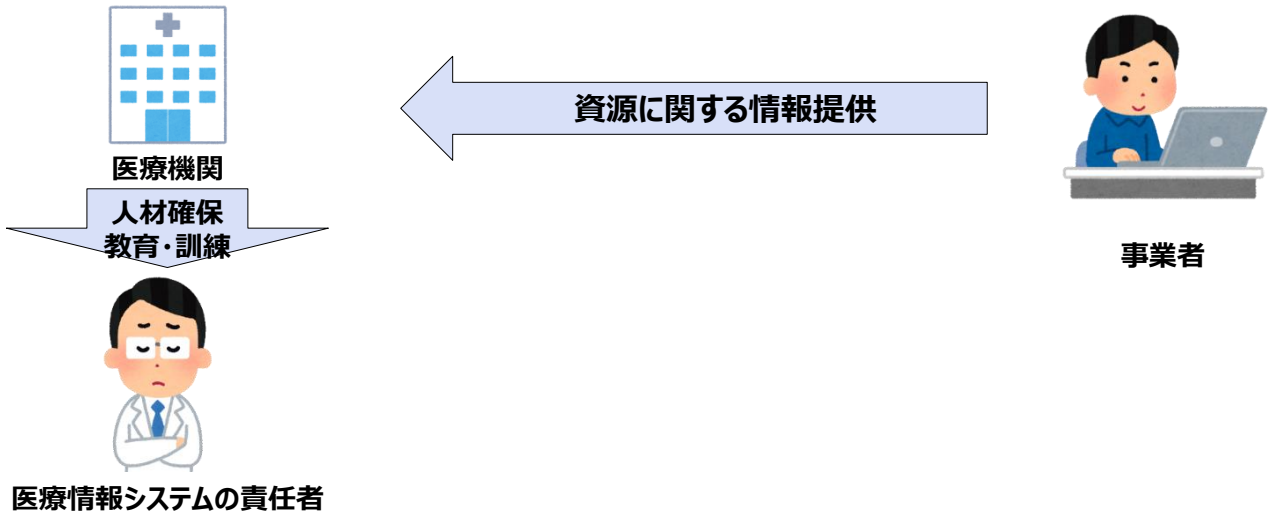
■ 個人情報の安全管理に関する職員への教育・訓練の実施及び実施状況に係る報告 【Part1 B3②】

(a) 職員が安全管理に関して遵守すべき内容を十分理解できるよう、教育や非常時に向けての訓練を定期的に行う。

(b) サイバー攻撃被害により地域医療の安全性を脅かされる近年の事案等を参考に、職員への教育を実施する。

■ 医療情報システムのセキュリティに関する情報提供義務【Part2 A11】

医療機関は医療の専門家であって、セキュリティについての専門性は乏しい場合が多いのに対し、専門的な医療情報システム等を提供する事業者は、セキュリティに関する専門的な知識・経験・人材を擁しているべきであり、こうした専門性の格差に鑑みて、事業者は、医療機関に対し、委託契約又は信義則に基づく付随義務として、医療機関が患者に対する安全管理義務を履行するために必要な情報を、適時適切に提供する義務（説明義務）を負うとされる。契約においては、説明義務の範囲を明確にし、医療機関にとって適時適切な情報提供がなされるよう、こうした事業者の説明義務の対象や内容をなるべく具体的な形で取り決める。



課題④：医療機関が管理する資源において、一部の資源に対する脆弱性対策が、他の資源の可用性に影響を与える可能性がある場合に、安全性の判断ができない。

■ 脆弱性情報の確認・報告 【推奨される対応例 Part2 参考1】

医療情報システムに関連する新たなセキュリティ上の脆弱性について、(独) 情報処理推進機構（IPA）等が公表する情報その他の情報を継続的に収集すること（又は合理的な範囲で収集に努めること）、および脆弱性発見時の医療機関への報告や対策の実施を行うこと等を取り決める。

■ ＯＳやアプリケーション、ハードウェアの保守の実施 【推奨される対応例 Part2 参考6】

システムを構成する機器、ソフトウェア、クラウドサービス等については、保守契約に基づき事業者による保守（セキュリティパッチの適用等）がなされるよう取り決める。オープンソースソフトウェア等の汎用ソフトウェアを使用する際も、脆弱性情報等のチェックやその対応についても取り決める。

■ セキュリティ対策の見直し提案 【Part2 A12】

情報セキュリティの最新情勢に鑑みて、安全管理上必要であれば、事業者において自発的に対策の見直しを行い、医療機関に提案することを取り決める。