「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」の利用手引

～医療情報システムのサイバーセキュリティに係る「契約」上の基本的な留意事項～

特定非営利活動法人
デジタル・フォレンジック研究会
「ヘルスケア」分科会

2024年11月

目次

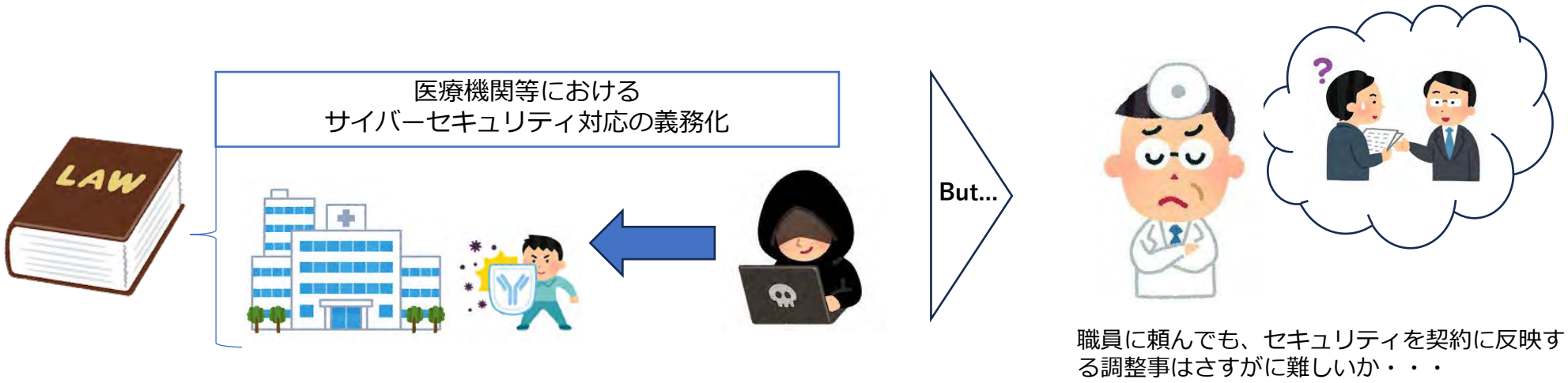
１.本手引きの背景・位置づけ

1．本手引きの背景・位置づけ(1/5)

2023年4月に医療法施行規則14条2項、及び薬機法施行規則11条2項一において、病院や調剤薬局（以下、「医療機関等」）におけるサイバーセキュリティが医療安全管理の一部として義務化されることになり、その対応に際しては厚生労働省『医療情報システムの安全管理に関するガイドライン』（以下、「厚労省GL」)を参照とすることが定められた。

厚労省GLでは、医療機関等は経済産業省・総務省『医療情報を取り扱う情報システム・サービスの提供ITベンダにおける安全管理ガイドライン』（以下、「2省GL」）も踏まえた観点より、医療情報システム・サービス（以下、「医療情報システム等」）を提供するITベンダ（以下、「ITベンダ」）との間でセキュリティの取り決め事項を契約等で合意することが求められている状況である。

しかしながら、**医療機関等の多くでは、セキュリティに精通した立場で、ITベンダとの契約交渉の中で具体的に契約条項の中にセキュリティ要件が含まれていることをチェックし、ITベンダと合意形成していくことは、特に専門的な知見の制約上、困難である**といえる。



1．本手引きの背景・位置づけ(2/5)

加えて未だ多くの医療機関等では医療情報システム等のセキュリティ管理について、ITベンダとの間での認識齟齬を抱える状況である。

特に規模が小さく、IT管理人材もいない医療機関等では、医療情報システム等の管理業務を全面的にITベンダに任せていることが多い。しかしながら、そうした条項が契約書には明確に定められていない限り、当たり前だがITベンダはそうした要求に適切に応答することは不可能であり、**そうした視差がセキュリティ責任の空白地帯をもたらすこと**になる。

こうした医療機関等/ITベンダ間という、**異なる業界間の認識ギャップが、国内医療機関等で多発するランサムウェア被害原因の大きな割合を占めている**点への理解は不可欠である。

医療機関等の立場

- ITベンダが提示するひな形の契約書等を吟味することなく、医療に携わるのであれば、あうんの呼吸で、**自分たちがやってほしいと思うシステム関連業務をベンダがすべて実施しているはずと思い込んでしまう。**
- システムの保守・運用にとどまらず、適切なセキュリティ実装・対応も含めてITベンダがすべて何も言わずとも担当してくれているという、**ITベンダも＜医の倫理＝暗黙のプロフェッショナリズム＞を求める姿勢。**

セキュリティ面の契約をめぐる認識ギャップ

発生

ITベンダの立場

- ITベンダはあくまで**契約書に基づくサービス提供しか実施できない**
- **契約内容にセキュリティ面が明記されていなければその対応自体が難しい**（契約にないことを勝手にやるわけにはいかない）

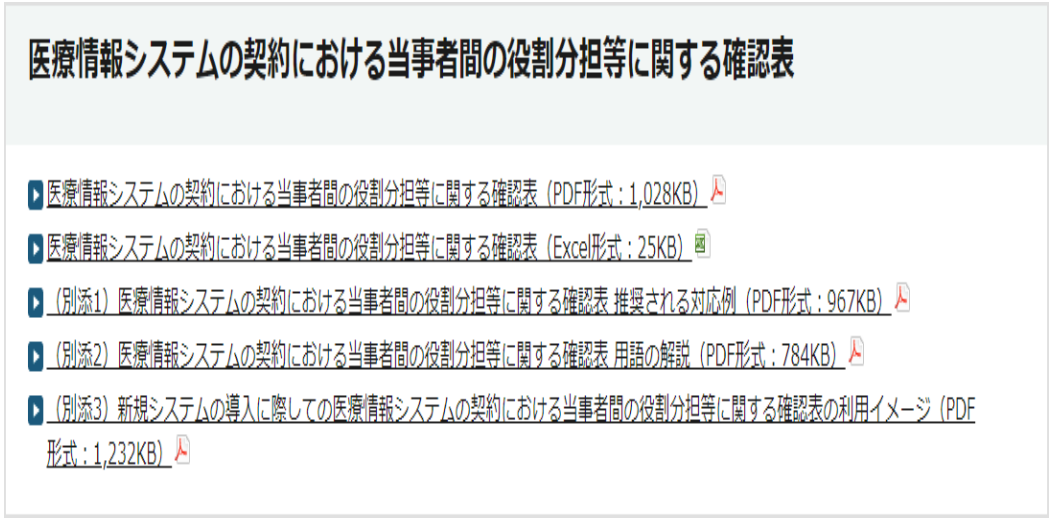
攻撃者が標的とするセキュリティの＜責任空白地帯＞

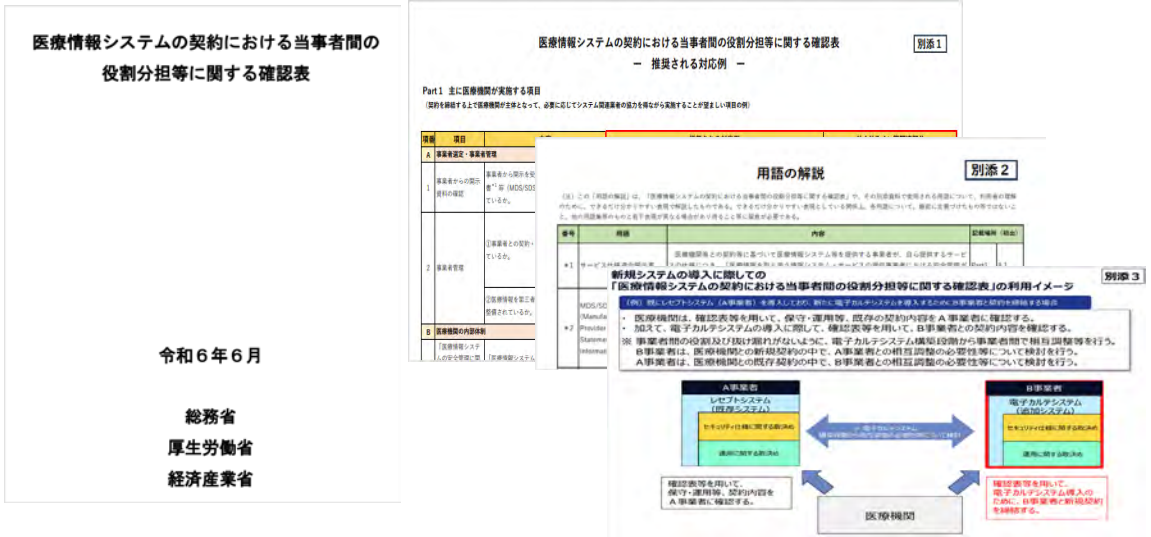
1．本手引きの背景・位置づけ(3/5)

こうした状況を是正すべく、2024年6月に、厚生労働省・経済産業省・総務省から、**『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』（以下、「契約検討確認表」）という、厚労省GL/2省GLに関する追加資料**が公表された。

契約検討確認表ではITベンダとの契約調整において、医療機関等/ITベンダの役割分担等を協議するために必要な項目について、医療機関等の確認ポイント、及び医療機関等がITベンダと共同で確認すべきポイントが整理され、それぞれにおいて推奨される対応事項が示されている。

本資料は、 ITや法務面の専門職員のいない医療機関等にとって、**医療情報システム・サービスをめぐるITベンダとの「情報の非対称性」を解消し、セキュリティ面の契約上の合意形成を適切に進めるうえで、非常に有益な資料**と考えられる。





https://www.meti.go.jp/shingikai/mono_info_service/medical_information_system/checklist.html

1．本手引きの背景・位置づけ(4/5)

ただし、契約検討確認表は、医療情報システム・サービスに係るセキュリティについて、契約上の合意形成を検討するための確認ポイントを示す構成となっており、**具体的に契約文言としてどのような条項を定めるかについては医療機関等で個別対応することが求められている**。

システム・サービスの提供形態、あるいは相対するITベンダによって多種多様となる契約形態を網羅する、常に正解となる契約内容は存在しないため致し方がないことではあるが、IT・法務面に詳しくない医療機関等にとっては、**もう一歩踏み込んだ、具体的な契約内容を検討する上でのヒント**が望まれるものと想定される

■契約検討確認表～本確認表の使い方（抜粋）

２．本確認表の使い方

○　本確認表の主な対象は、マルチベンダー型契約により役割分担等が複雑であるものの、法務やITに精通した担当者が不在である中小規模の病院を想定している。小規模な診療所等では対象外となるような項目が含まれているが、適切に選択すれば有用と考えられる（※）。

（※）例えば、小規模な診療所等では、担当する業務ごとに区分された組織（部署）がなく、組織運営のための計画等がない場合がある。このような場合は、厚労省ガイドライン別添小規模医療機関向けガイダンスを参考にして、必要な内容を定めることが重要である。

～～（中略）～～

④　最終的には、医療機関と事業者との間で協議した結果を、できるだけ具体的な文言で合意形成文書に落とし込むことを想定する。

なお、本確認表は、医療機関や事業者の責任を一義的に定めることを目的として作られたものではない。

具体的な契約文言として、
どういった点に気を付ければいいのか・・・

1．本手引きの背景・位置づけ(5/5)

上記の背景を考慮し、当研究会「ヘルスケア」分科会の第21期ワーキンググループでは、**契約検討確認表の実務面における＜使いやすさ＞をサポート**すべく、厚労省GL/2省GLを踏まえた観点より、**ITや法務の専門人材のいない小規模な医療機関等**が、医療情報システム・サービスを提供するITベンダとセキュリティ面の責任分界を合意形成するに際して、**契約書の中でどのような具体的な文言・内容に着眼して検討を行うべきかについての情報**を提供することにした。

また、実際に契約面でセキュリティ事項の取り交わしがない状況下で事故が発生した際に**ITベンダ側の過失が認められた裁判例の概説**、および**医療機関等が業界固有の慣習として把握しておくべきITベンダ側の制約情報等**、実際にITベンダと契約を進める上で参考になる関連情報を補足としてあわせて示すことで、医療機関等が契約検討確認表に基づくITベンダとの契約調整・交渉をサポートすることを本手引きの位置づけとする。

「ヘルスケア」分科会
第21期ワーキンググループ

支援

想定読者層：「ITや法務の専門人材のいない小規模医療機関等」

契約条項で重点的に
着眼すべき要件の概説

事前に
把握しておきたい
関連情報

実現

契約検討確認表を活用したITベンダとの契約調整の円滑化

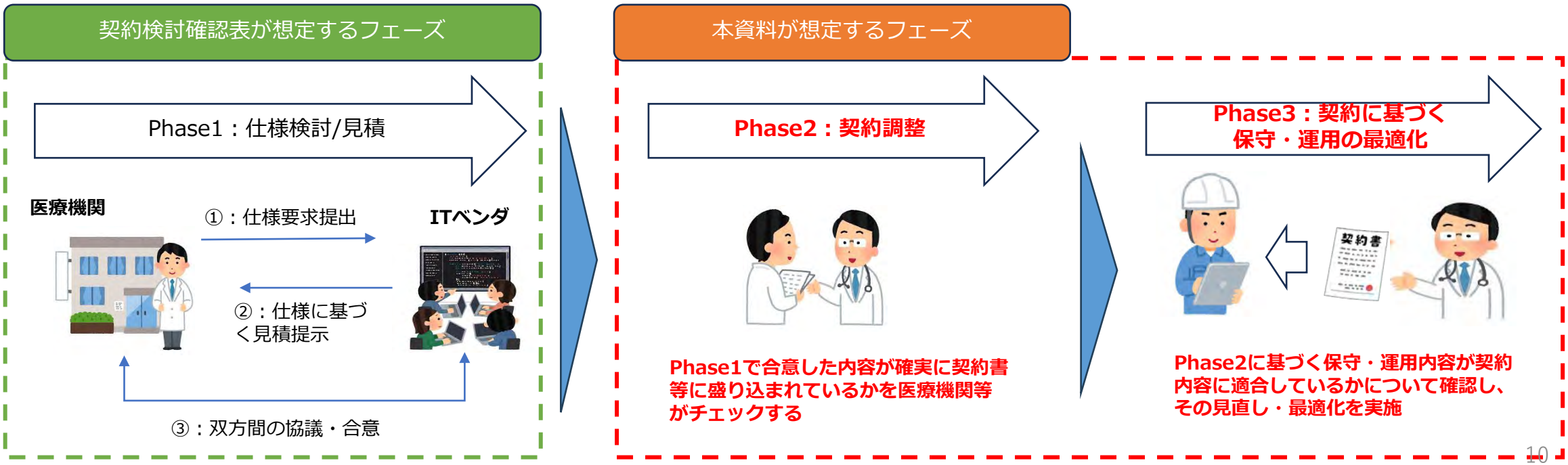
２.契約上の具体的な文言を検討する際の考え方

2．前提(1/3)～検討の正しいタイミング

医療機関等/ITベンダをめぐる医療情報システム等の導入までのコミュニケーションは、医療情報システム等の機能要件/非機能要件（セキュリティ面）を含む機能・運用仕様を双方が協議・合意するフェーズ（Phase1）、機能・運用仕様の合意結果に基づく観点より、契約書の具体的な文言調整を行うフェーズ（Phase2）、そしてPhase2で締結した契約に基づき保守・運用が行われるフェーズ（Phase3)に一般的に分類可能である。

契約検討確認表を補足することを目的とした本資料は、あくまでPhase1にて契約検討確認表に基づく適切な調整がITベンダとの間で行われたことを前提にした観点より、**その後のフェーズ（Phase2/Phase3)において契約上の具体的な文言の調整、あるいは見直しを実施する際の検討上の観点を示すことを目的**としている。

よって、Phase1において適切な取組を、契約検討確認表に基づき実施したうえで、本資料を利用することが推奨される。

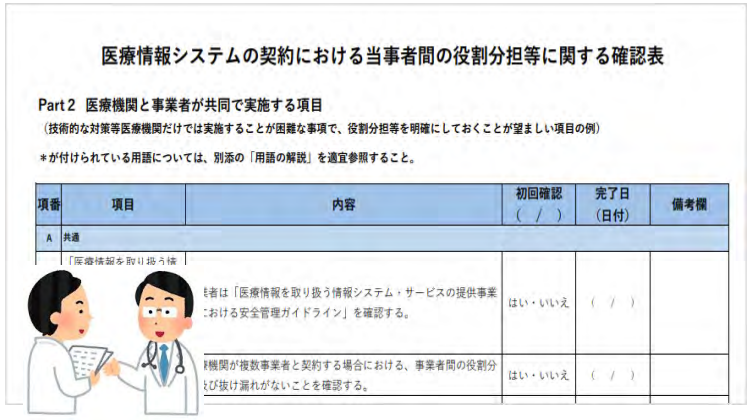


2．前提(2/3)～全体像（1/2）

本章では、前頁を前提としたうえで、契約検討確認表のうち、医療機関等がITベンダと共同で確認を行うPart2（『2．医療機関とITベンダが共同で実施する項目』）を対象として、実際に契約書の文言の具体的な検討・協議を行うなかで、医療機関等において、特に着眼すべきテーマを、**<A．管理ルールの可視化>、<B．環境変化の適時把握>、<C. リスクコミュニケーションの依頼>、<D. 責任の前提の明確化>**として整理し、ITベンダによる標準的な契約文言イメージ、医療機関等が見直す文言イメージ・意図等の解説を通して、契約に定めるべき要件を具体化した形で概説している。

本手引きを参考にすることで、**ITや法務に詳しくない医療機関等においても、契約検討確認表に基づく確認作業の中で、医療情報システム等のセキュリティに係る契約をどのような切り口で検討すべきかを、一定の具体的なイメージとして掴むことが可能になると思われる。**

ただし、本章の内容は法的な助言や保証を企図するものではなく、あくまで契約文言等も検討時の着眼点を示す位置づけで提示している。実際の契約書の最終的な文言の確定にあたっては、専門の弁護士に依頼することが不可欠である。


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

Part 2　医療機関と事業者が共同で実施する項目

（技術的な対策等医療機関だけでは実施することが困難な事項で、役割分担等を明確にしておくことが望ましい項目の例）

＊が付けられている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認（　/　）	完了日（日付）	備考欄
A	共通				
	「医療情報を取り扱う情				
		者は「医療情報を取り扱う情報システム・サービスの提供事業における安全管理ガイドライン」を確認する。	はい・いいえ	（　/　）	
		機関が複数事業者と契約する場合における、事業者間の役割分及び抜け漏れがないことを確認する。	はい・いいえ	（　/　）	

契約検討確認表 /
Part 2　医療機関とITベンダが共同で実施する項目

インプット


A.管理ルールの可視化


B.環境変化の適時把握


C.リスク
コミュニケーション


D.責任の前提の明確化

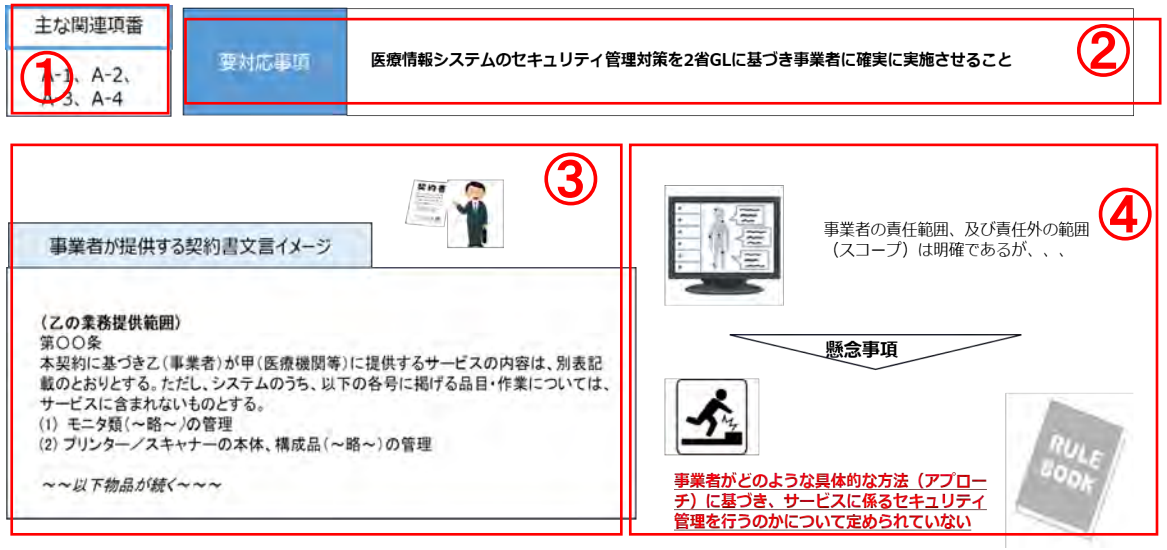
4つの切り口より、契約文言の具体的なイメージを提示

寄与

医療機関等の担当者が、ITベンダと調整・交渉する際にどのような切り口で、契約書の文言にセキュリティ要件を反映すべきかの具体的イメージ把握

2．前提(3/3)～凡例（2/2）

次頁以降の構成は以下の凡例を参照。

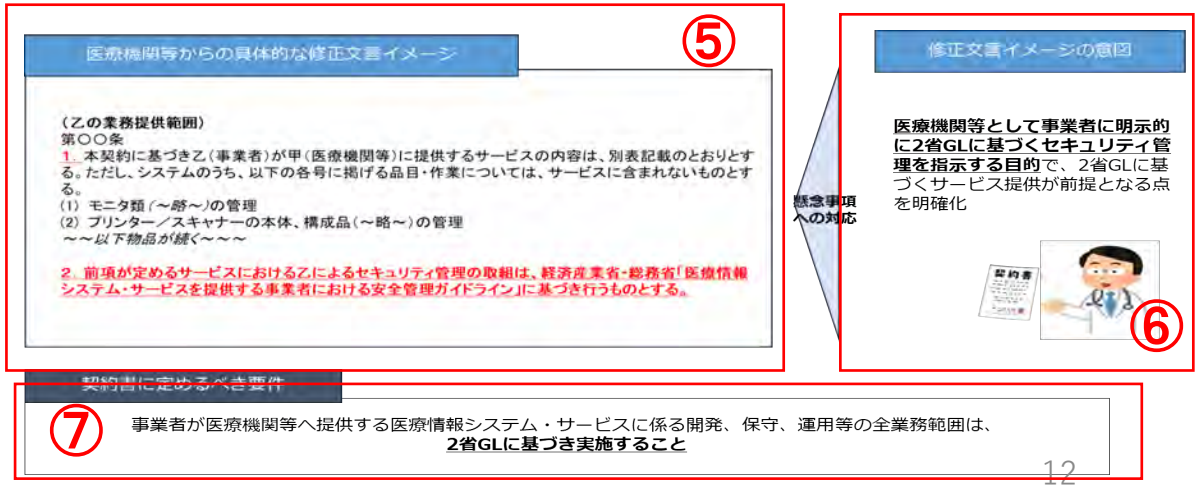


①：[主な関連項番]
契約検討確認表のうち、[Part２ 医療機関とITベンダが共同で実施する項目]の関連番号を記載

②：[要検討対応事項]
①の項番要件を踏まえ、医療機関等がITベンダとの契約調整のなかで達成すべき目標を記載

③：[ITベンダが提供する契約書文言イメージ]
①に関する範囲のなかで、ITベンダが標準的に提供する契約文言例・イメージ等を記載

④：懸念事項
③のうち、医療機関等にとって、①・②を踏まえた場合、対応すべき内容を記載



⑤：[医療機関等からの具体的な修正文言イメージ]
③に対して、④を踏まえた観点から、医療機関等として契約内容に定めるべき、修正・更新文のイメージ例を記載

⑥：[修正文言イメージの意図]
⑤の文言をなぜ定めるべきかについての説明等を記載

⑦：[契約書に定めるべき要件]
医療機関として、ITベンダと①を共同確認するなかで、ITベンダに対して契約書に定めることを要求すべき内容のサマリー

A：管理ルールの可視化(1/2)

主な関連項番	要対応事項	
A-1、A-2、 A-3、A-4	要対応事項	**医療情報システムのセキュリティ管理対策を2省GLに基づきITベンダに確実に実施させること**

ITベンダが提供する契約書文言イメージ

（乙の業務提供範囲）
第〇〇条
本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。ただし、システムのうち、以下の各号に掲げる品目・作業については、サービスに含まれないものとする。
(1) モニタ類（～略～）の管理
(2) プリンター／スキャナーの本体、構成品（～略～）の管理

～～以下物品が続く～～～

ITベンダの責任範囲、及び責任外の範囲（スコープ）は明確であるが、、、

懸念事項

ITベンダがどのような具体的な方法（アプローチ）に基づき、サービスに係るセキュリティ管理を行うのかについて定められていない

A：管理ルールの可視化(2/2)

医療機関等からの具体的な修正文言イメージ

（乙の業務提供範囲）
第〇〇条
1. 本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。ただし、システムのうち、以下の各号に掲げる品目・作業については、サービスに含まれないものとする。
(1) モニタ類*（～略～）*の管理
(2) プリンター／スキャナーの本体、構成品（～略～）の管理
～～以下物品が続く～～～

2. 前項が定めるサービスにおける乙によるセキュリティ管理の取組は、経済産業省・総務省「医療情報システム・サービスを提供するITベンダにおける安全管理ガイドライン」に基づき行うものとする。

懸念事項への対応

修正文言イメージの意図

医療機関等としてITベンダに明示的に2省GLに基づくセキュリティ管理を指示する目的で、2省GLに基づくサービス提供が前提となる点を明確化

契約書に定めるべき要件

ITベンダが医療機関等へ提供する医療情報システム・サービスに係る開発、保守、運用等の全業務範囲は、
2省GLに基づき実施すること

B：環境変化の適時把握(1/2)

主な関連項番	要対応事項	
A-５、A-10、A-12		**①：ITベンダによる医療情報システムのセキュリティ管理態勢・環境・手順の変更が発生した場合、医療機関等に対して適時に内容報告を行い、承認を得ること** **②：業務の再委託を行う場合は、医療機関等の事前承認を不可欠とするとともに、再委託先のセキュリティ面を含めた管理監督責任は全てITベンダが担うこと**

ITベンダが提供する契約書文言イメージ

（変更の通知）
第〇条
本契約は甲（医療機関）・乙（ITベンダ）双方が記名捺印した書面によってのみ変更することができるものとする。

（再委託）
第△条
乙（ITベンダ）は、業務提供範囲の全て又はその一部を第三者に委託することができるものとする。

懸念事項①

変更があった場合は契約見直しを行う定めがあるが、**どのような範囲・水準での変更があった場合、契約見直しするかについての定めがない**

懸念事項②

仮に再委託がITベンダにより行われても、**医療機関等はその事実を把握できず、厚労省GLに基づく、委託先としての管理監督責任を遂行できない**

B：環境変化の適時把握(2/2)

医療機関等からの具体的な修正文言イメージ

（変更の通知）
第〇条
1. 本契約は甲（I医療機関）・乙（ITベンダ）双方が記名捺印した書面によってのみ変更することができるものとする。
2. 前項のうち、本契約で定めた乙の業務提供範囲のうち、甲のセキュリティ管理態勢へ影響を及ぼす変更が発生する場合は、契約変更予定日の●●日以内に予め乙が甲へ通知し、甲の承認をもって変更するものとする。

（再委託）
第△条
1. 乙（ITベンダ）は、業務提供範囲の全て又はその一部を**甲（医療機関等）による事前同意のもとで、**第三者に委託することができるものとする。
2. 乙は第三者への委託に際して、乙と同等のセキュリティ管理義務を第三者に求め、その状況を管理監督する責務を有する。
3. 乙が委託した第三者において義務違反があった場合、当該義務違反は乙の義務違反とみなすものとする。

修正文言イメージの意図

懸念事項①への対応

ITベンダと取り交わした業務提供内容について、契約締結後に未許可の変更が発生し、**医療機関等へ想定外の影響・問題が生じることを予防する目的**で、事前に指定した期間内に通知することを明確化。

懸念事項②への対応

ITベンダが知らぬ間に再委託先に医療機関等の患者情報等も含めた管理委託を行うことを予防する目的で、ITベンダが再委託する場合は、委託元（ITベンダ）は医療機関等に事前同意を得ること、及び再委託先の管理監督責任は全てITベンダが担うことを明確化

契約書に定めるべき要件

再委託先への業務委託等も含め、ITベンダによるサービス提供内容・体制の変更が発生する場合、
医療機関等は委託元としての管理責任を果たすため、その変更状況を適時かつ適切に把握できるプロセスをITベンダに整備させること

C：リスクコミュニケーションの依頼(1/2)

主な関連項番	要対応事項	
A-11		**ITベンダに対して、2省GLに基づく医療情報システム等を利用するに際して、医療機関等として当該システム等に実装された機能を用いて、厚労省GLが求めるユーザセキュリティをどのように実施すべきかについての情報提供依頼（リスクコミュニケーション）を行うように求めること**

ITベンダが提供する契約書文言イメージ

（乙の責任）(※) *※ (A)修正文文言イメージと同一内容*
第〇条
1. 本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。
（～略～）
2. 前項が定めるサービスは、経済産業省・総務省「医療情報システム・サービスを提供するITベンダにおける安全管理ガイドライン」に基づき行うものとする。

（甲の乙に対する協力）
第◇条
1. 甲（医療機関等）は乙（ITベンダ）が本件システムのサービスを円滑に行えるよう万全を期し、次の各号に従い乙に協力するものとします。
（～略～）
2. 前項に定めたサービスに必要な補助（電気・照明・通信回線、リモートメンテナンス用機器、及び消耗品）を甲の責任のもとで提供するものとする。

懸念事項①

ITベンダによる保守サービス（リスクマネジメント）は2省GLに基づく定めがあるが、**医療機関側で実施すべきセキュリティ面の対応事項に関する情報提供という、リスクコミュニケーションの定めが十分でない**

懸念事項②

保守サービスの実施に向けた医療機関等の協力範囲のうち、**医療機関等としてどのようなセキュリティ対策を行うべきかについて、ITベンダとの責任分界が十分でない**

C：リスクコミュニケーションの依頼(2/2)

医療機関等からの具体的な修正文言イメージ

（乙の責任）
第〇条
1．本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。
（～略～）
2．前項が定めるサービスにおける乙によるセキュリティ管理の取組は、経済産業省・総務省「医療情報システム・サービスを提供するITベンダにおける安全管理ガイドライン」に基づき行うものとする。
3．前二項のサービスにおけるセキュリティ実施事項のうち、甲が管理する範囲・内容については、乙主導のもと、甲が為すべき具体的な事項を甲乙間で協議のもとで、決定・実施するものとする。

懸念事項①への対応

（甲の乙に対する協力）
第△条
1．甲（医療機関等）は乙（ITベンダ）が本件システムのサービスを円滑に行えるよう万全を期し、（～～～略～～）
2．　前項に定めた保守サービスに必要な補助（電気・照明・通信回線、リモートメンテナンス用機器、及び消耗品）を甲の責任のもとで提供するものとする。
3．前二項の保守サービスにおける甲の責任となる提供物に係るセキュリティ対応事項は、乙主導のもとで、甲乙が協議した結果に基づき、甲により実施されるものとする。

懸念事項②への対応

修正文言イメージの意図

ITベンダに対して2省GLに基づくリスクコミュニケーションの取組に明示的にコミットさせる目的で、医療機関が医療情報システム等の利用に際したユーザセキュリティの実施内容について、2省GLに基づき、ITベンダが情報提供・サポートを主導的に行うなかで、両者が協議した結果に基づき、医療機関の責任で実施する点を明確化

契約書に定めるべき要件

ITベンダが提供する医療情報システム等の中で、2省GLに基づき、**医療機関等が行うべきユーザセキュリティをITベンダが情報提供し（リスクコミュニケーション）、サポートする**こと

（補足）リスクコミュニケーションを通して依頼すべき情報提供・サポート事項の対象範囲

契約書に定めるべき要件

ITベンダが提供する医療情報システム等の中で、2省GLに基づき、**医療機関等が行うべきユーザセキュリティをITベンダが情報提供し（リスクコミュニケーション）、サポートする**こと

契約確認表 Part2

契約検討時に最低限求めるべき具体的な情報提供・サポート事項の対象範囲

B.システム導入契約

1.利用者認証
2.通信相手の認証
3.通信経路に対する安全対策の確保
4.暗号化
5.ネットワーク構成
6.品質確保の状況

C.システム保守・運用契約

1.ネットワークのトラフィック監視
2.機器運用監視
3.運用委託先によるシステムの管理状況の報告
4.事故発生時の報告
5.事故発生時の原因究明・対策

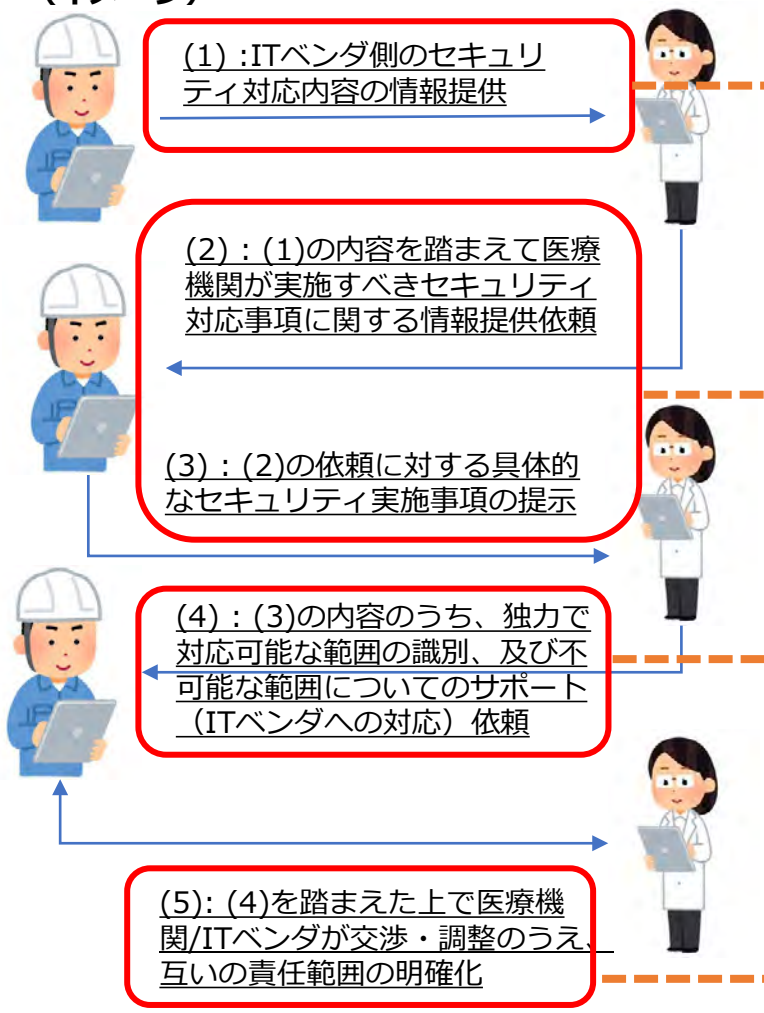
このシステムを実際に使う場合、具体的にどんなセキュリティ対策を行えばよい？？

ポイント

契約検討確認表Part2における「B.システム導入契約」、「C.システム保守・運用契約」が定める各項番の要求事項について、医療機関等が対応を行うために具体的にどのようなセキュリティ面の取組を行うべきか（医療機関等としての責任範囲はどこまでか）を明確化することが重要！
（「よくわからないけど、確認表に基づいてITベンダと共同でチェックしたんだから大丈夫だろう」という考え方はNG）

（補足）情報提供・サポート事項の識別に向けた一般的なフローイメージ

■契約検討確認表 Part2における医療機関/ITベンダ共同確認の一般的フロー（イメージ）



■契約確認表 /Part2 - B.システム導入契約 -5 ネットワーク構成の要求事項を例にした場合の、医療機関等の具体的なアクション

Part2 B.システム導入契約 -5. ネットワーク構成における要求事項

診療等に必要なネットワークを適切に構築する。

① ITベンダ側が担うネットワーク構築においてどのようなセキュリティ対策が2省GLの観点より行われているかに関する情報提供依頼を行うこと

② 構築されたネットワーク環境のうち、医療機関等が厚労省GLの要件を踏まえ、どのようなセキュリティ管理を具体的に行うべきかについての情報提供依頼を行うこと

③ ②を検討した結果、医療機関等の独力で対応できない事項のうち、ITベンダへのサポート・対応依頼を行う範囲の識別

④ ネットワークを適切に構築するに際した、医療機関等/ITベンダ相互の責任範囲を調整・交渉のうえ明確にし、契約締結をすること

ポイント

契約書には契約確認表part2の共同確認結果に基づく、責任範囲の明確化までのやり取りを別紙として含めることも一案である（明示的に合意形成した証跡を契約書別紙として記録管理する）

D：責任の前提の明確化(1/3)

主な関連項番	要対応事項	
A-1、A-3、A-11	要対応事項	**2省GLに基づく観点より、医療機関等として最低限求めるセキュリティの前提条件（善管注意義務の範囲）を明確化したうえで、ITベンダ側の免責や損害賠償責任等の範囲を定めるようにすること**

ITベンダが提供する契約書文言イメージ

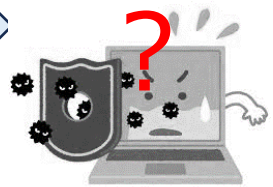
第●条（損害賠償責任の範囲）
(1)甲（医療機関等）は、乙（ITベンダ）の契約違反により損害を受けた場合に限り、通常の損害について損害賠償を請求できるものとします 。ただし、相手方に請求できる損害賠償の範囲には、天災地変やその他の不可抗力により生じた損害、または甲の責に帰すべき事由により生じた損害は含まれないものとします。
(2)乙（ITベンダ）はいかなる場合においても、甲（医療機関等）の逸失利益および第三者から甲に対してなされた賠償請求に基づく損害については責任を負わないものとします
（～～以下略～～）

第〇条（免責）
乙（ITベンダ）は以下の各号の事由について責任を負いません
(1)乙の指定外の各種ソフトウェア、OS等を利用したことによって生じる故障・障害
(2)甲（医療機関）の指示により乙が実施した事項による故障・障害
（～～以下略～～～）

懸念事項①

医療機関の逸失利益、第三者による損害賠償請求等に係るITベンダの免責は、**「いかなる場合」でも一切の例外なく適用されるのか？**

懸念事項②



ITベンダが指定したソフトウェアやOSに脆弱性が発生し、それに適時にパッチを適用した結果の故障や障害は医療機関の責任になるのか？

D：責任の前提の明確化(2/3)

医療機関等からの具体的な修正文言イメージ

（乙の責任）
第〇条
1. 本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。
（～略～）
2. 前項が定めるサービスにおける乙によるセキュリティ管理の取組は、経済産業省・総務省「医療情報システム・サービスを提供するITベンダにおける安全管理ガイドライン」に基づき行うものとする。
3. 前二項のサービスにおけるセキュリティ実施事項のうち、甲が管理する範囲・内容については、乙主導のもと、甲が為すべき具体的な事項を甲乙間で協議のもとで、決定・実施するものとする。

第●条（損害賠償責任の範囲）
1. 甲（医療機関等）は、乙（ITベンダ）の契約違反により損害を受けた場合に限り、通常の損害について損害賠償を請求できるものとします 。ただし、相手方に請求できる損害賠償の範囲には、天災地変やその他の不可抗力により生じた損害、または甲の責に帰すべき事由により生じた損害は含まれないものとします。
2. 乙（ITベンダ）はいかなる場合においても、甲（医療機関等）の逸失利益および第三者から甲に対してなされた賠償請求に基づく損害については責任を負わないものとします
3. 前2項は、乙に故意又は重過失がなく、第〇条第2項における乙の適切な取組が行われている限りにおいて適用されるものとし、乙による当該取組の不備に伴い、損害および利益逸失が発生した場合、乙は甲と誠実に協議のうえ、逸失利益も含めた適切な賠償を行うものとします

懸念事項①への対応

修正文言イメージの意図

ITベンダ側の業務提供範囲（乙の責任）において2省GLに基づくセキュリティ管理の取組を前提とする旨を記載し、当該取組をITベンダの善管注意義務として位置付ける。（【C：リスクコミュニケーションの依頼】を参照）

そのうえで、**医療機関/ITベンダ間における賠償責任範囲の前提を明確にする目的**で、ITベンダによるセキュリティ管理の取組において、仮に善管注意義務へ違反した場合、**損害賠償請求の免責事項には該当しない点（故意・重過失の要件に該当する点）**を明示。

契約書に定めるべき要件

ITベンダが提供する医療情報システム等の中で、2省GLに基づく適切なセキュリティ管理の取組を行うことを、
業務上の責任範囲（善管注意義務）として明確に指定し、そのうえで免責条件を定義すること

D：責任の前提の明確化(3/3)

医療機関等からの具体的な修正文言イメージ

（乙の責任）
第〇条
1. 本契約に基づき乙（ITベンダ）が甲（医療機関等）に提供するサービスの内容は、別表記載のとおりとする。
（～略～）
2. 前項が定めるサービスにおける乙によるセキュリティ管理の取組は、経済産業省・総務省「医療情報システム・サービスを提供するITベンダにおける安全管理ガイドライン」に基づき行うものとする。
3. 前二項のサービスにおけるセキュリティ実施事項のうち、甲が管理する範囲・内容については、乙主導のもと、甲が為すべき具体的な事項を甲乙間で協議のもとで、決定・実施するものとする。

第〇条（免責）
1. 乙（ITベンダ）は以下の各号の事由について責任を負いません
(1)乙の指定外の各種ソフトウェア、OS等を利用したことによって生じる故障・障害
(2)甲（医療機関）の指示により乙が実施した事項による故障・障害
（～～以下略～～～）
2. 本条第1項(1)については、乙に故意又は重過失がなく、第〇条2項における乙の適切な取組のもとで、乙が指定した各種ソフトウェアやOS等に脆弱性が発生した場合、同条3項において、乙主導のもと、甲が実施すべきセキュリティ実施事項を甲乙協議のもとで決定・実施する取組が適切に行われる限りにおいて適用されるものとします。なお、甲乙協議の頻度は乙が甲と協議のうえで決定するものとします。

懸念事項②への対応

修正文言イメージの意図

懸念事項①への対応同様、ITベンダによるセキュリティ管理は2省GLに基づき実施することを前提として位置付ける。

そのうえで、**ITベンダが指定したソフトウェアやOS等に脆弱性が発生した場合の対応を厚労省GLに準じる観点より行っていく仕組みを整備する目的**で、ITベンダが指定したソフトウェア類等の脆弱性対応に係る大方針を明示。
　なお、具体的な脆弱性対応等の頻度は別途協議して決定とすることで、一定のフィージビリティを確保

契約書に定めるべき要件

ITベンダが医療情報システム等の利用に際して指定したソフトウェア/ハードウェアに脆弱性が発生した場合、
ITベンダ起点で脆弱性への対策を医療機関等へ協議・相談する仕組みの整備

3.補足情報

(a)：裁判例から見る契約上のセキュリティ責任～前提

第2章「契約上の具体的な文言を検討する際の考え方」において、医療機関等が医療情報システム等の導入、保守・運用契約を結ぶ上で検討すべきセキュリティ対応事項を、ITベンダが提供する一般的な契約文言イメージをベースとして、医療機関等として修正依頼を行うべき要件を示した。

ただし、実際の紛争では、**セキュリティについての契約の文言は曖昧・概括的**であることが多い。また、契約に明記されていなくとも、**損害（情報漏洩等のセキュリティ・インシデント）の原因となったセキュリティ対策上の不備について、その対策が一般的になされるべき事項であれば、ITベンダーの義務違反（過失）と判断され、損害賠償が認められるケースも存在**する。

ここでは、ある裁判例を通して、**契約面でセキュリティに関する明示的な取り交わしがなくとも、ITベンダの責任が認められた事例を概略的に紹介**する。

こうしたケースの存在も頭に入れた上で、ITや法務に詳しい担当者がいない医療機関等では、どのような姿勢でITベンダとの契約調整に臨むかについて考えることが必要である。

(a)：裁判例から見る契約上のセキュリティ責任(1/2)

＜東京地裁平成２６年１月２３日判決・判例時報２２２１号７１頁＞

事例概要

- ECサービスを提供するA社が、ITベンダのB社に対して、自社のウェブサイトで商品受注システムの開発等の委託契約を締結。
- B社が開発したウェブサイトには**SQLインジェクション対策が十分でないという脆弱性**があり、**委託契約完了後の期間**において、その脆弱性を悪用したサイバー攻撃が発生。
- その結果、A社に商品注文を行った顧客のクレジットカード情報の漏えいが発生。**本来はクレジットカードをウェブサイト側で保管すべきでなく、保管する場合は暗号化が必要だったが**、その措置も行っていなかったことも原因。
- A社は、こうした不備のあるシステムの納入を行ったB社に対して、**債務不履行に基づく損害賠償請求**を行った。

債務や損害賠償について定められた契約条項（意訳）

【損害賠償に係る条項】
B社が委託業務に関連して、**B社又はB社の技術者の故意又は過失**により、A社若しくはA社の顧客又はその他の第三者に損害を及ぼした時は、B社はその損害について、A社若しくはA社の顧客又はその他の第三者に対し賠償の責を負うものとする。

【損害賠償の制限条項】
前項の場合、B社は**個別契約に定める契約金額の範囲内において**損害賠償を支払うものとする。

A社は、セキュリティ対策の不備を5つ挙げて、債務不履行（過失）を主張してB社の責任を追及
B社は、債務不履行を争うとともに、責任制限条項の適用を主張した

(a)：裁判例から見る契約上のセキュリティ責任(2/2)

①：SQLインジェクション対策	過失あり

- B社は、当時の状況下で、ECウェブサイトシステムの発注を受けたのだから、**その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていた**と考えるべき。
- 当時は**SQLインジェクションによる情報漏洩被害が多発**しており、経済産業省やIPAが、ウェブサイトのSQLインジェクション**対策の重要性を繰り返し啓発・公表**していた
- 上記の状況を前提に、**SQLインジェクション対策としてバインド機構の使用又はエスケープ処理を施したプログラムを提供する債務を認定**

②：カード情報の暗号化	過失なし

- IPAが重要データは暗号化保存することが望ましい旨を公開・公表していた
- ただし、**「望ましい」という努力義務の水準での要求事項であり**、システムパフォーマンス見合いで検討すべき事項等の留保条件もあるため、**暗号化対策を行わなかったこと自体は過失なしとされた**

責任制限条項	適用には故意・重過失が必要

- 個別契約の金額を損害賠償の上限とする責任制限条項について、故意又は重過失がある場合にまでこれを適用することは、**著しく衡平を害するものであって、当事者の通常の意思に合致しない**（解釈により契約書に書いていない要件を加重）
- 本件についての重過失の有無について検討し、①専門業者であるB社の**注意義務は比較的高度**であること、②経産省・IPAが代表的攻撃手法としてSQLインジェクションについて注意喚起していたこと、③**対策は容易**だったこと、を根拠に重過失があると認定
- 責任制限条項の適用を否定

本判決は契約時点の技術水準の観点から見て、当然実施されているべきセキュリティ対策について、**契約書に記載がなくとも、黙示的に合意があった**として、ITベンダの義務違反（過失）と認定した。
また、損害賠償の制限条項についても、記載のない重過失を要件として付加し、ITベンダの重過失を認めた。

(b)：ITベンダから見える景色～前提

第2章「契約上の具体的な文言を検討する際の考え方」はあくまで医療機関等の目線で記述されているため、一見すると、医療情報システム等を提供するITベンダはあたかも医療機関等を食いものにする「悪者」であるかのごとく記されている。
しかしながら、**これは医療機関等の立場で見た場合のイメージである点には留意すべきである。**

【本手引きの背景・位置づけ】でも示した通り、医療機関/ITベンダには構造的な認識ギャップがある。これは公定価格を基にした社会福祉としての医療を担う業界と、資本主義的な市場価格を前提とした民間事業体という、国内の業界固有の差異による考え方の違いに起因するといえる。
当然だが、ITベンダはあくまで契約書に基づくサービス提供しか実施できず、契約内容にセキュリティ面が明記されていなければその対応自体も難しい。
さらにいえば、その対応を行う場合、ITベンダは**追加的なコストを病院へ求めねばならない**ため、民間企業に医の理念を元にコストカットを求めることは慎まなければならない。

以上より、医療情報システム等を提供するITベンダが、**医療機関等が忌避する<コスト>を前にして、いかに医療機関等におけるセキュリティ対応の前で足踏みをせざるを得ない状況が発生しているかについて、実際のITベンダの事例をもとに紹介**する。

本資料ではこうした事例を通して、厚労省GLが示す通り、何故「セキュリティとは経営層が関与すべき投資である」のかについて、医療機関等にも理解してもらえればと思う。

(b)：ITベンダから見える景色(1/2)～セキュリティ対策の逆説

医療機関等と具体的にコミュニケートしているITベンダが実際に体験した事例を以下に紹介する。

事例１

ITベンダのA社から、**情報セキュリティ管理強化の目的で導入した**グループウェアシステムの運用管理を別のITベンダであるB社が引き継ぐことになった。
B社が引き受けた対象システムはすでにメーカサポートが終了した旧いOS上で動作していたため、B社はOSのアップデート依頼の検討を医療機関等へ行った。しかし、アップデートに伴う動作検証等には**数百万近く**を要し、予算を確保できないという理由から、旧いOSでの運用継続がB社に指示された。
B社としては、このままA社が構築したシステムの運用管理継続を行い、旧いOSの脆弱性に起因したセキュリティインシデントがあった場合、**結果的に本来、医療機関等が当初目指していた情報セキュリティ管理の目的と乖離することになるのではないかと心配している**。

事例2

あるITベンダのC社では、統合脅威管理(Unified Threat Management）ソフトウェアを医療機関等へ導入し、保守サービスを提供しているが、保守契約の金額を削減したいという医療機関等の意向により、ソフトウェアのバージョンアップを行うことは契約対象外としている。
様々なセキュリティ関連の外部機関から該当ソフトウェアの脆弱性の情報が発出されてるため、C社は医療機関等に脆弱性対応を行うべきである旨、それは**数十万程度の有償対応**になる旨を伝えた。
しかし、医療機関等からは予算がないため、対応不要との回答があり、実質的に、**脆弱性のある統合脅威管理ソフトウェアによる運用が該当機関ではいまも行われている状況である。**

**セキュリティ対策のために導入したシステムや製品の更新や保守に係る「投資」を医療機関等が嫌った結果、
セキュリティ上の＜穴＞を逆説的に作ることに繋がっている**

(b)：ITベンダから見える景色(2/2)～非対称関係に伴う課題

事例３

ITベンダのD社は、医療情報システム・サービスへ不審なアクセスログの分析・評価機器の導入・運用業務を提供している。
ある医療機関等に対して機器導入後の実効的なログモニタリングに向け、ログ上の異常検知・調査・対応といった運用業務に**毎月50万程度が必要**である見積もりを提示した。
しかしながら、当該医療器機関は、費用の高さに加え、「機器の導入＝セキュリティの確保が実現された」と誤解し、**そうした分析業務を「無駄なコストの押し売りである」として拒否した。**
そのため、機器の運用に伴う実効的なログモニタリングのプロセス構築までにはたどり着かず、当該医療機関では、**導入した機器を形式的に運用しているだけのサービスで満足している状況**である。

事例4

あるITベンダE社は、ある医療機関等に対して、医療情報システムのログを平時に取得・保存・モニタリングするという運用業務を引き受けていた。
しかしながら、当該医療機関等におけるサイバーインシデントの発生に伴い、ログの保全やデジタルフォレンジック等の追加作業を引き受けることになり、それに伴う**追加費用を請求したが、これらは既存の運用業務の契約に含めるべきとして当該医療機関に押し切られ、請求は棄却**された。
E社は対象医療機関との付き合い方を再検討している状況である。

医療機関等/ITベンダ間で「セキュリティ」を理解するための業務慣習・目線等のフレームワークの違い（非対称性）が、こうした基本的な意思疎通上の課題をもたらすことになっている

Appendix：ワーキンググループ参加メンバーリスト

本手引きを作成した「ヘルスケア」分科会の第21期のワーキンググループメンバーは以下の通り。

氏名	所属
江原 悠介	分科会主査　PwCJapan有限責任監査法人 リスクアシュアランス ディレクター
緒方 健	分科会幹事　(共)情報・システム研究機構 人工知能法学研究支援センター 特任研究員
吉峯 耕平	分科会幹事　田辺総合法律事務所 パートナー弁護士
舟橋 信	分科会幹事　（株）セキュリティ工学研究所 取締役、（株）FRONTEO 取締役
和田 則仁	分科会幹事　神戸大学大学院　医学研究科　医療創成工学専攻　特命准教授
近藤 剛	有徳綜合法律事務所 弁護士
鈴木 文一朗	（株）ワイ・イー・シー 取締役
小野 健太郎	（株）ワイ・イー・シー 取締役