「医療機関におけるサイバーセキュリティ確保事業」

規約

第 1.0 版

厚生労働省

改版履歴

版数	年月日	主な内容	備考
第1.0版	2024年7月3日	制定	

目次

1.　本規約の目的 3

2.　定義 3

3.　役務内容 3

4.　免責事項等 5

5.　禁止事項 5

6.　本役務の変更、中止等 6

7.　秘密保持 6

8.　知的財産 6

9.　損害賠償 6

10. 規約改定 6

11. 本規約上の地位の譲渡等 7

12. 紛争解決 7

別添　医療機関におけるサイバーセキュリティ確保事業前提条件

1. 本規約の目的

令和 6 年度「医療機関におけるサイバーセキュリティ確保事業」（以下「本事業」という。）の実施にあたり、厚生労働省（以下「当省」とする）は、「医療機関におけるサイバーセキュリティ確保事業規約書」（以下「本規約」という。）」について定め、これにより医療機関に対する調査及びバックアップ体制の整備支援（以下「本役務」という。）」を提供する。本医療機関（2-1 で定義するものをいう。）は、本役務の提供を受けるにあたって、本規約に同意する。

2. 定義

2-1. 用語の定義

用語	用語の意味
本医療機関	本役務の提供を受ける医療機関。
管理者	本役務を提供する上で、当省および受託事業者との窓口を担う本医療機関の担当者。
調査拠点	医療機関が指定する、本役務の提供を受ける拠点。
現地調査	調査拠点のシステム構成等を把握するための現地調査。
調査報告書	本事業における調査結果の本医療機関向け報告書。

3. 役務内容

当省は、本医療機関に対して、無償で、「病院の外部ネットワーク接続の俯瞰的把握、安全性の検証・調査」（以下「本セキュリティ調査」という。）及び「病院のオフラインバックアップ体制の整備支援」（以下「本バックアップ整備支援」という。）を提供する。なお、当省は、本事業の遂行にあたっては、東日本電信電話株式会社（以下「受託事業者」という。）に対して、本医療機関に対する本役務の提供業務を委託する。また、受託事業者は、本医療機関に対する本役務の提供業務の一部を第三者に再委託する場合がある。

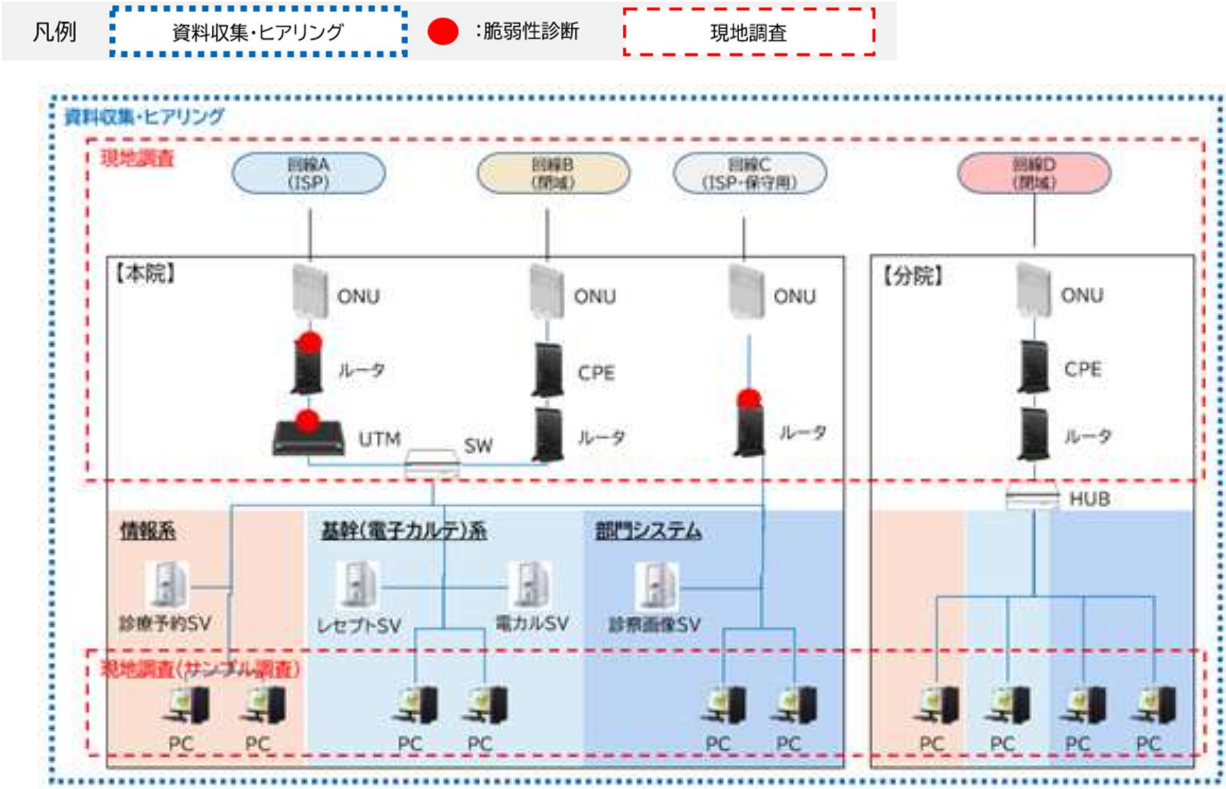
3-1. 病院の外部ネットワーク接続の俯瞰的把握、安全性の検証・調査

受託事業者は、本医療機関の医療情報システムに接続する外部ネットワーク接続点を俯瞰的に把握した上、そのネットワークに係るセキュリティ対策状況を調査する。受託事業者は、本セキュリティ調査後、調査報告書（当省指定のフォーマット）を作成する。調査範囲・手順及び報告項目は、以下別記の通りを予定するが、詳細は別途開催する病院向け説明会にて説明をする。

[別記 1] 調査範囲・手順

本セキュリティ調査における調査対象は、基幹（電子カルテ）系と接続されている全ての外部接続点、及びその周辺のルーター、FW、PC 等の一部機器とする。なお、基幹（電子カルテ）系につながらないネットワークは調査対象範囲外とする。

調査にあたっては、院内ネットワーク構成に関する関連資料を管理者から受領したうえで必要に応じてヒアリングを実施し、事前の協議と日程調整を踏まえて、現地調査及び脆弱性診断を実施する。セキュリティ調査にあたって、提出を求める書類は別表 1 の通りとする。



［別表１］調査にあたって医療機関から提出を求める資料一覧

資料名	フォーマット	シート名	詳細説明	Check
①医療機関依頼（回線・機器情報等記入）.xlsx	当社提供フォーマット	基本情報記入シート	【記入必須】 • 記入をお願いします。	□
		回線・機器情報記入シート	【記入必須】 • 記入をお願いします。	□
		調査端末情報記入シート	【記入必須】 • 記入をお願いします。	□
		設置場所記入シート	【記入必須】 • 調査対象機器の設置場所を平面図またはフロア図にプロットしたうえでご提出をお願いします。	□
②ネットワーク概要図	病院様フォーマット	ー	【可能であれば】 • 既存資料がありましたら、調査の参考とさせて頂くためご提供をお願いします。	□

［別記２］調査結果の報告

本セキュリティ調査を実施した後、定型の報告書を作成し医療機関に対して報告する。報告事項は以下の通りを予定するが、詳細は別途開催する病院向け説明会にて説明をする。

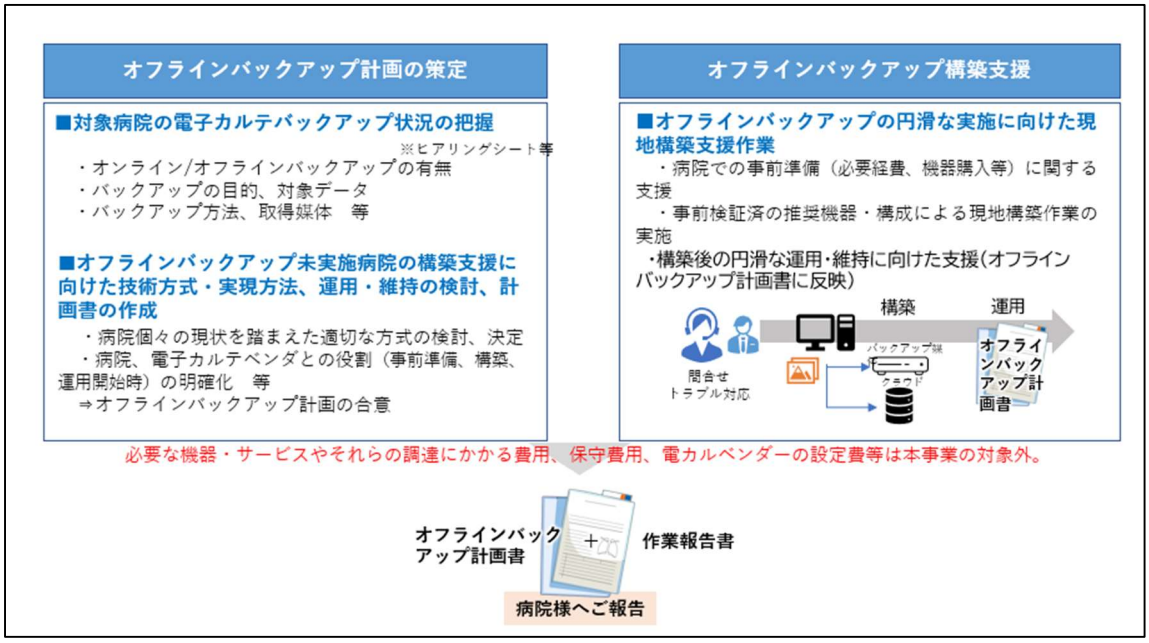
- 調査で判明した外部接続ネットワーク概要図
- 脆弱性診断結果
- とるべきセキュリティ対策案

3-2. 病院のオフラインバックアップ体制の整備支援

受託事業者は、本医療機関の医療情報システムを対象としたオフラインバックアップ実施に係る支援を行う。

受託事業者は、本バックアップ整備支援にあたり、本医療機関が用意するバックアップソフト、RDX 等の設置・設定・試験、簡易報告書の作成支援を行う。なお、本事業に係る機器調達および機器保守・運用は役務の対象外であり、医療機関の負担にて用意することとする。バックアップの対象は電子カルテシステムとし、バックアップデータの出力は原則として本医療機関、又は本医療機関が委託するベンダーが実施する。概要は以下別記の通り予定するが、詳細は別途開催する病院向け説明会にて説明をする。

[別記]オフラインバックアップ体制の整備支援の概要について



本医療機関は、必要に応じて事前に受託事業者と打合せを行い、現状のバックアップ形式の情報共有や、オフラインバックアップシステムを構築するにあたっての方式などについて協議、合意する。

免責事項等

本医療機関は、受託事業者が別添「医療機関におけるサイバーセキュリティ確保事業前提条件」に記載された事項を前提として本役務を提供することを確認する。当省は、本医療機関が本役務に基づき取得又は利用する一切の情報の内容の最新性・適時性・正確性・完全性については保証しない。

4. 禁止事項

本医療機関は、本役務の提供を受けるにあたり、以下の各号のいずれかに該当する行為をしてはならない。当省は、本医療機関が以下の各号に該当する又は該当するおそれがあると判断した場合、事前の通知をすることなく、本規約に基づく本役務の提供を取りやめることができ、これによって本医療機関に生じた損害について責任を負わない。

(1) 法令に違反する行為、法令違反を助長する行為又はそれらのおそれのある行為

(2) 公序良俗に反する行為

(3) 当省又は受託事業者その他第三者の知的財産権、肖像権、プライバシーの権利、名誉、その他の権利又は利益を侵害する行為
(4) その他、当省による本事業の実施を妨害するおそれがある又は本規約及び本事業の趣旨・目的に反する等当省が不適切と判断する行為

5. 本役務の変更、中止等

当省は、本医療機関に事前の通知をすることなく、本役務の内容の全部又は一部を変更又は提供を中止することができる。

6. 秘密保持

当省、受託事業者及び本医療機関は、本事業にあたり知り得た秘密情報を、本事業のためのみに使用し、かつ相手方の同意なく第三者に開示又は漏洩しないものとする。ただし、次の各号いずれかに該当する情報は除く。

(1) 開示されたときに相手方が知得していたもの
(2) 開示されたときにすでに公知であったもの
(3) 開示された後で相手方の帰責事由なく公知になったもの
(4) 開示の権限を有する第三者から、秘密保持の義務を負うことなく、適法に知得したもの
(5) 本医療機関名を特定しない形で利用されるもの

上記の義務は、本役務の終了後３年間存続する。

7. 知的財産

本事業の過程で生じる発明、考案又は創作について、特許権、実用新案権、意匠権、商標権、著作権等の知的財産権は、当省に帰属する。本事業において受託事業者が本医療機関ごとに作成する報告書については、本事業の目的の範囲内において、当該本医療機関において無償で利用することができる。

8. 損害賠償

当省は、本役務の遂行に起因又は関連して本医療機関に損害等が発生した場合においても、重大な過失がない限り賠償する責任を負わない。また、当省が仮に賠償する責任を負う場合であっても、その責任は、当該違反によって現実に生じた通常の直接損害の範囲に限るものとし、いかなる場合であっても、逸失利益その他特別損害に係る責任は負わないものとする。

本医療機関は、当省又は受託事業者に対して不正確な情報を提供することその他故意又は過失に基づく行為によって、当省、受託事業者又は第三者に損害を与えた場合には、本医療機関が自らの費用及び責任において事案の解決にあたるとともに、当該損害（紛争解決に要した弁護士費用及び人件費を含む）を補償する。

9. 規約改定

当省は、以下の各号のいずれかに該当する場合、本医療機関の承諾を得ることなく、本規約を変更できるものとする。

(1) 変更内容がサービス名や表現の変更又は誤字、脱字の修正等であり、本規約の内容に実質的に影響しない場合
(2) 変更内容が本医療機関の一般の利益に適合する場合
(3) 変更内容が契約をした目的に反せず、かつ、変更の必要性、変更後の内容の相当性その他変更に係る事情

に照らして合理的なものである場合

当省は、上記第 2 号及び前項第 3 号による変更の場合、本規約変更の効力発生の相当期間前までに、本規約を変更する旨及び変更後の本規約の内容並びにその効力発生時期を受託事業者のウェブサイト等への掲載その他当省が適当と判断する方法により公表又は通知する。

10. 本規約上の地位の譲渡等

本医療機関は、本規約上の地位又は本規約に基づく権利義務の全部又は一部を、第三者に対する譲渡、承継（合併、会社分割等による包括承継を含みます。）し、又は担保の目的に供することはできない。

11. 紛争解決

本規定に定めのない事項及び本契約の履行又は解釈にあたって生じた疑義について、信義誠実の原則に従い、その都度協議により定めるものとする。本規約の準拠法は日本法とし、本規約に起因し又は関連する一切の紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所とする。

以上

別添　医療機関におけるサイバーセキュリティ確保事業前提条件

病院の外部ネットワーク接続の俯瞰的把握、安全性の検証・調査

- 本医療機関は本事業の主旨や規約を理解したうえで調査へ協力する
- 本医療機関への現地調査は平日日中帯（9 時～17 時）を基本とする。別途、リモートで実施する調査（脆弱性診断等）については、夜間も含めて事前におおよその実施日時を取り決める。
- 調査にあたって、管理者は 2024 年 9 月 30 日までに資料提出や調査日程の確定などに協力する
- 現地調査は、別途調査に要する日数を提示するが、想定した日数で調査完了しなかった場合、継続調査のため改めて調整を行い、追加調査する可能性がある
- 本医療機関内における調査については、本医療機関関係者の立ち合い、拠点内の写真撮影許可、管理者又は本医療機関関係者による端末機器等の操作、作業者からの問合せ対応といった協力を必要とする。
- 作業可能な範囲は、高さ 2 メートルまでの脚立を利用して手が届く（又は、そこから目視できる範囲）とする。予備機器が保管されている場合は、受託事業者の判断で可能な範囲で調査を実施することとする。
- 事前に調査に必要な情報（回線情報、端末ログイン情報等）が医療機関から開示されず不明のままであった場合、調査報告においては不明な旨記載し調査を完了する。また、調査当日に新たに発覚した機器やネットワークについては調査対象範囲外とする。
- 調査の際、医療機関等の機器操作等で何らか不具合や不明点が生じた場合、医療機関の関係者に対して問合せや報告を行う。
- 事前に定めた調査手法に基づいて実施した作業に関連して、偶発的に発生したトラブル等の復旧は本事業の責任範囲外とする。
- 脆弱性診断の実施にあたっては、受託事業者の示す「脆弱性診断実施における注意事項」（別紙）を参照し、同意の上で診断を行うこととする。
- 医療機関都合による調査日程の変更については、予定日から 7 営業日前までに受託事業者へ申告を行うこととする。7 営業日を割り込んでの日程再調整には応じられない可能性がある。

病院のオフラインバックアップ体制の整備支援

- オフラインバックアップの対象は、電子カルテシステムのみとする。
- 電子カルテシステムのバックアップデータの出力は、医療機関又は電子カルテベンダが実施することとする。
- オフラインバックアップ媒体の要件は以下を満たすものとする（予定）

（ア）ネットワーク経由でのバックアップ媒体への保存又は PC に接続されたバックアップ媒体への保存が可能であること。

（イ）バックアップ媒体は、オンライン/オフラインの切り替えが可能、もしくは追記不能設定が為されている仕組みであること。

（ウ）3 世代以上のバックアップデータの保存が可能であること。

（エ）外部クラウド又は外部データセンターにバックアップデータの保存が可能であること。

■　作業工程は 3 日間を予定する。平日日中帯を基本とする。

■

■　以下の作業は対応範囲外とする

(ア) 医療機関保有のシステムに対する作業

(イ) 医療機関ごとの個別設定値の設計、医院個別手順書の作成

(ウ) 資材購入（バックアップソフト、バックアップ媒体機器等）

(エ) サービス契約(クラウドへのオフラインバックアップサービス)

(オ) 院内 LAN スイッチへの追加設定

(カ) データ(dump ファイル)の吐き出し

(キ) 作業後の電子カルテ動作確認

(ク) オフラインバックアップデータを用いた院内システムのリストア作業・リストア試験

(ケ) 作業後の医療機関都合による追加作業(設定変更等)

(コ) 完了後の保守運用対応

■　受託事業者にバックアップサーバの構築を依頼する場合、医療機関にて準備対応する内容は、以下の通りとする

(ア) 現地作業前に受託事業者、医療機関、電子カルテベンダとの打合せを設定し、設定情報や作業時の注意事項、工程やヒアリングしたい内容について合意する

(イ) 作業にあたり、医療機関は、以下の取り組みを行う

（a）受託事業者が設置するバックアップサーバ・RDX・LTO テープドライブの設置スペースおよび電源、バックアップサーバ用の IP アドレスの払い出しおよび医療機関側のファイル出力されている機器とネットワーク的に通信可能な LAN ポート（1 口）の準備

（b）受託事業者が設置するバックアップサーバ必要なネットワーク設定（Window ドメイン参加、アカウント作成、Samba 関連設定、WSUS 設定、その他必要な設定など）情報の提供

（c）各医療機関ですでに導入している監視サーバや端末管理ソフトなどの登録

（d）受託事業者が設置するバックアップサーバへの出力するための医療機関側サーバ、ネットワーク機器監視サーバ等の設定変更

（e）医療機関側でのセキュリティポリシーに準拠し、ウィルス対策や端末管理ソフト等（医療機関側での費用負担を想定）の導入や設定変更等

（f）受託事業者が設置するバックアップサーバ内のバックアップ用フォルダへのアクセス確認

（g）受託事業者が設置するバックアップサーバとの疎通確認、バックアップデータの出力確認実施

（h）受託事業者が設置するバックアップサーバへのバックアップデータの出力完了時刻（目安）の通知および完了確認

（i）上記の連携、確認のための現地立ち合い

（j）受託事業者が作業をする際に不明な点がある場合、問合せに対応すること

(k)　予定した作業当日までに、医療機関側で各種機器・ソフトウェア一式の用意ができない場合、受託事業者での工事が実施できない場合がある