2024年7月3日（水）
厚生労働省　医政局　特定医薬品開発支援・医療情報担当参事官室　主催

厚生労働省「医療機関におけるサイバーセキュリティ確保事業」オンライン説明会
ご説明資料

東日本電信電話株式会社　ビジネスイノベーション本部

目次

1. 実施内容

事業概要

- **近年、国内外の医療機関を標的としたランサムウェア等のサイバーセキュリティインシデントが増加しています。医療機関のサイバーセキュリティ被害は、診療を長時間制限することによる地域医療への影響に加え、患者の個人情報が窃取される等の深刻な被害をもたらす可能性があり、サイバーセキュリティ対策の充実が喫緊の課題です。**
- **本事業は、実効性の高いセキュリティ対策として、①外部ネットワーク接続の俯瞰的把握、安全性を検証・調査、および②オフラインバックアップの整備支援の実施を行います。**

＜事業概要＞

①外部ネットワーク接続の俯瞰的把握、安全性の検証・調査

外部接続点やセキュリティ対策状況の洗い出し

ヒアリングシート

セキュリティ対策等の調査

現地調査、脆弱性診断

対象：　全病院

構成、脆弱性の見える化、対策提案

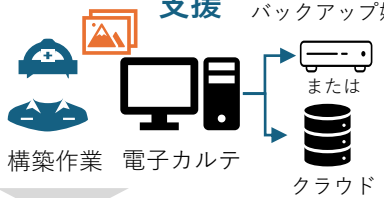
②オフラインバックアップの整備支援

オフラインバックアップ計画の策定

電子カルテバックアップ状況の把握、技術方式・実現方法、運用・維持の検討

対象：　オフラインバックアップ未実施の病院

オフラインバックアップ構築支援



オフラインバックアップ計画書

＜本事業による病院のメリット＞

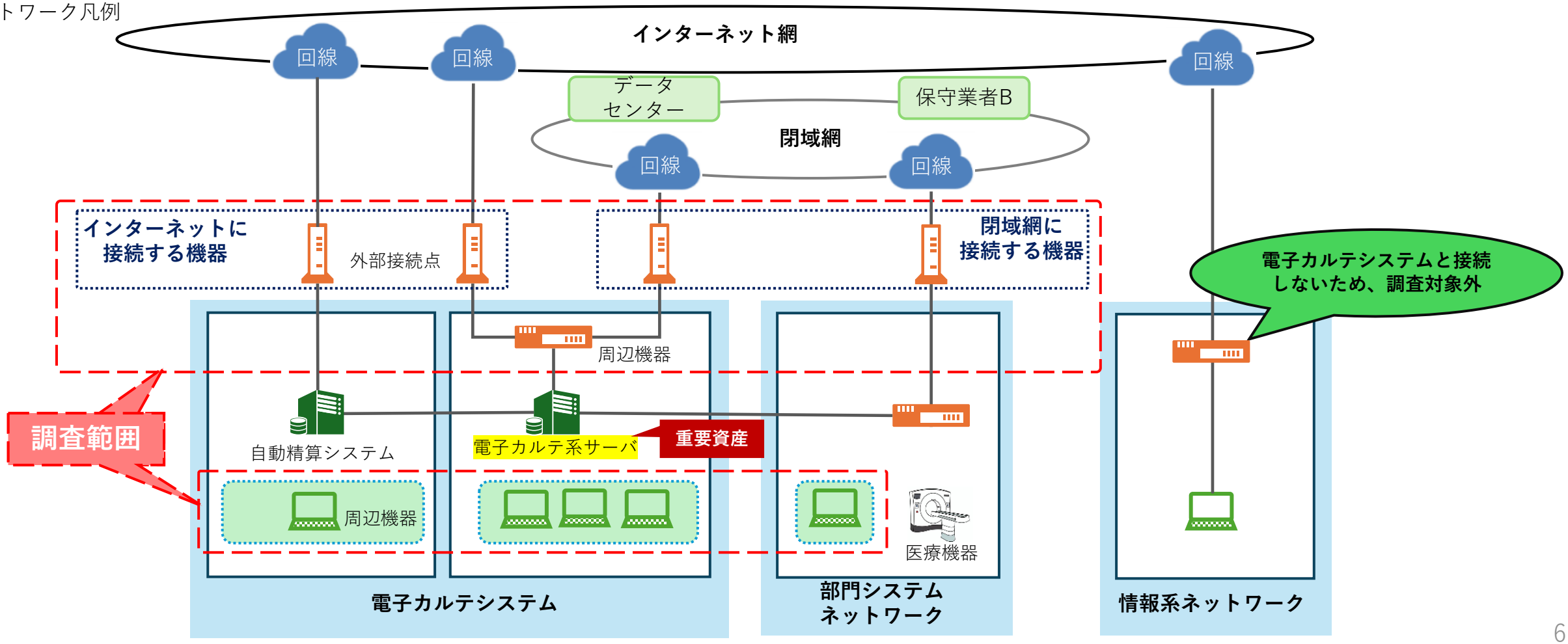
- 部門システムや医療機器の保守用回線を含め、外部接続点を網羅的に把握し、病院の管理下におくことが可能となります。それぞれの外部接続点の機器構成、および第三者の検証・調査を通じたリスクを見える化します。
- 電子カルテのオフラインバックアップ環境を整備することにより、万が一の際の電子カルテデータの保全が可能となります。また、オフラインバックアップ実施は、「診療録管理体制加算1」算定のための施設基準項目の一つになっています。

外部ネットワーク接続の俯瞰的把握、安全性の検証・調査

調査範囲

- **回線・ネットワーク機器・セキュリティ機器等の現況を確認し、俯瞰的把握に繋がる必要な情報を収集します。**
- **電子カルテと繋がる全ての外部接続点と、その周辺機器に重点を置いた調査範囲とします。電子カルテシステムと接続のないネットワークは対象外です。**
- **調査範囲に対して、①現地調査、②脆弱性診断の2つの工程を実施します。**

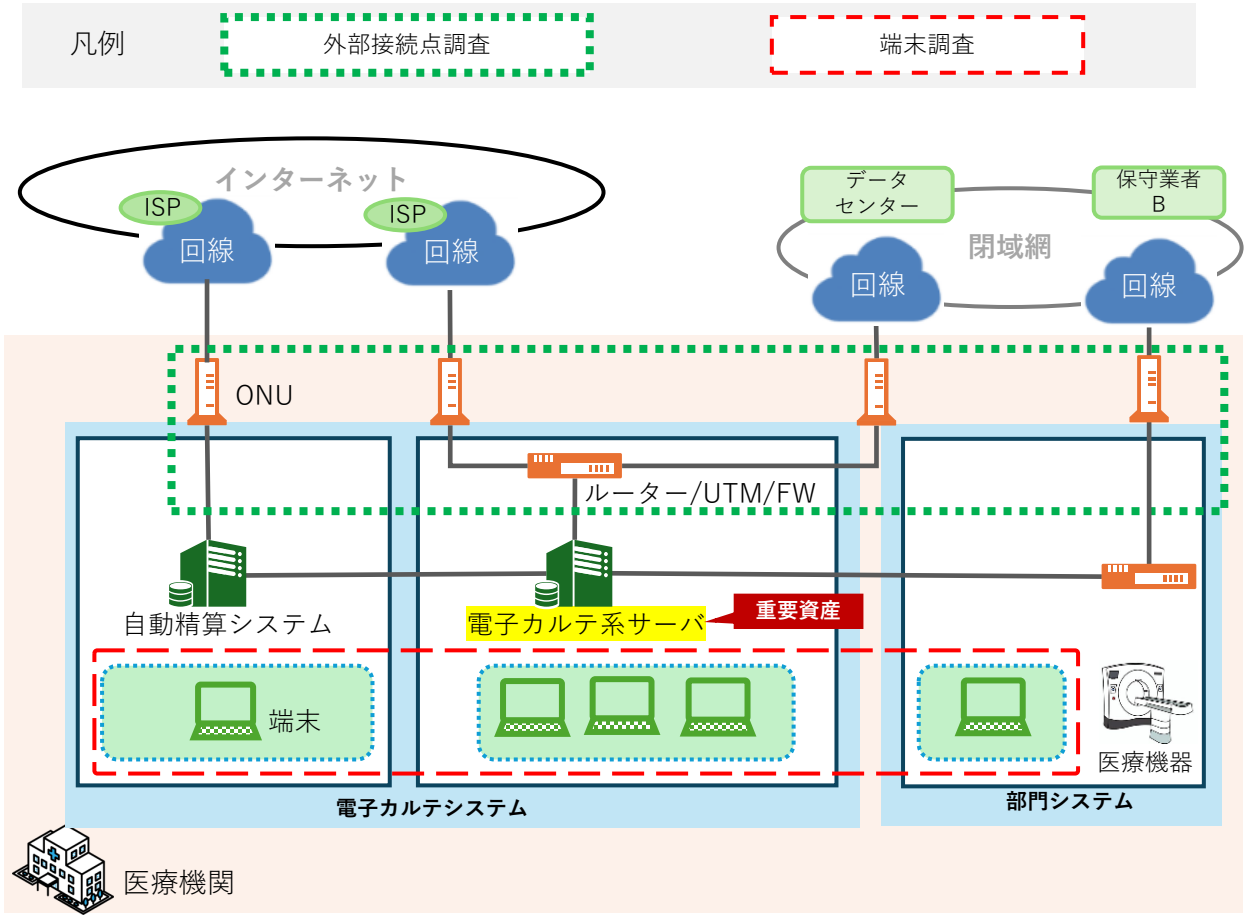
ネットワーク凡例



現地調査について

調査におけるポイント

- リモート保守用の回線や、閉域網、無線等、基幹（電子カルテ）系につながるすべての出入り口を調査対象とします。（電子カルテシステムから独立しているネットワークは調査対象外）
- 現地調査の前にお答えいただくヒアリングシートの回答内容に従って、ご希望いただいた端末に対してセキュリティ対策を確認します。（台数、機種の制限あり）

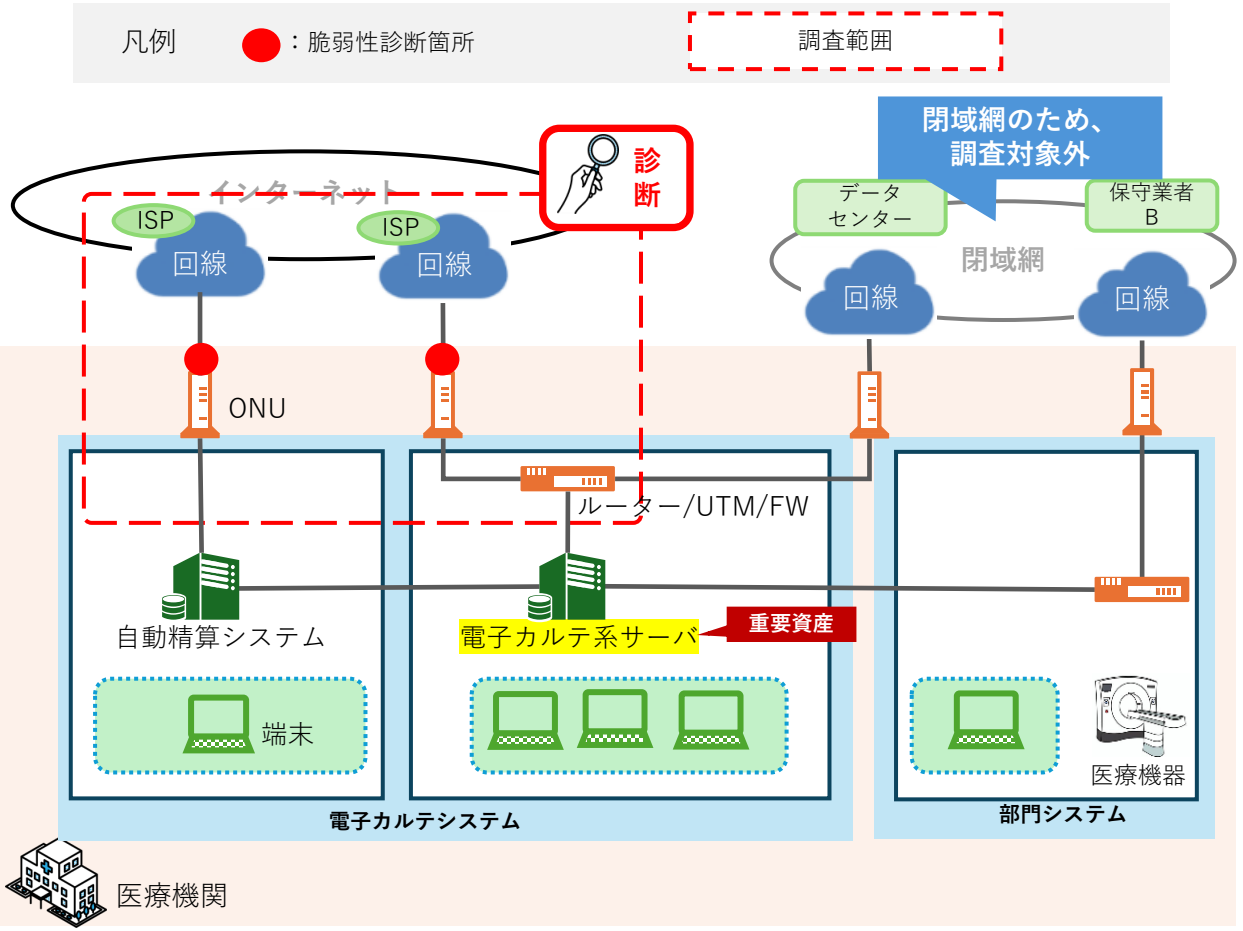


項目	内容
【調査目的】	外部接続点 • 病院の外部ネットワーク接続の俯瞰的把握、外部接続点の洗い出し
	端末調査 • 端末のセキュリティ対策状況の調査
【調査内容】	外部接続点 • 外部接続点を中心とした物理構成の把握 • 回線情報、ルータ情報の確認 • セキュリティ機器（FW/UTM/IPS/IDS等）の情報確認 • 対象機器（ルータ・UTM）のファームウェアバージョン等の確認
	端末調査 • 電子カルテおよび主要な部門システム端末のOS、ウィルス対策ソフトのバージョン、USB閉塞等の確認
【注意事項】	外部接続点 • 貴院で管理していない回線については、回線契約者にご協力いただく場合がございます（ベンダー名義等）。 • 対象機器の確認において、一部ファームウェアバージョン等を確認できない装置がございます。
	端末調査 • WindowsOSを対象として**5台**の調査を実施いたします。

脆弱性診断について

調査におけるポイント

- グローバルIPアドレスに対して、ポートスキャンを行い脆弱性診断を行います。
- インターネット接続のある回線が対象となり、閉域網に接続された回線は対象外となります。
- グローバルIPアドレスが動的の場合は診断当日にアドレスを改めて確認いただく必要があります。
  ※ご確認いただけない場合には調査不可となりますのでご注意ください。
- リモートでの診断となるため当日の立ち合いは不要です。



項目	内容
【診断目的】	• 外部接続点の脆弱性診断を実施し安全性の確認をする
【診断内容】 • ポートスキャン（TCP/UDP）	• 通信ポート応答確認 • インターネットからアクセス可能なポート（サービス）を調査。
【診断内容】 • 脆弱性スキャン（TCP/UDP）	• 脆弱性の調査 • 利用バージョンの調査 • バックドア診断 • アカウント診断 など
【備考】	• 脆弱性診断を実施する際は、対象装置のグローバルIPアドレスをお知らせください。 • ポートスキャンでアクセス可能なポートが見つかった場合、脆弱性スキャンを実施します。 • 脆弱性スキャンは、応答するポートに応じた診断を実施するため、上記全項目が診断される訳ではありません。

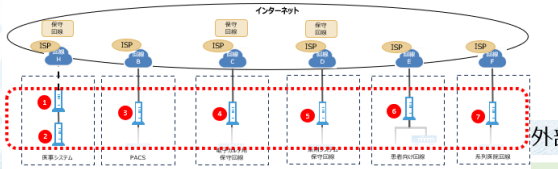
病院向け調査レポート

- **現地調査と脆弱性診断の結果をもとに調査結果をまとめ、レポートとしてご提出します。**
- **調査完了から1.5カ月後を目途にレポートを提出させていただく予定です。**
  ※下記の内容はサンプルとなります。実際の報告時には内容が変更となる可能性があります。

外部ネットワーク接続点　調査結果

外部ネットワーク接続点の見える化（1/2）

貴院の外部ネットワーク接続点を俯瞰的に見える化した結果は以下の通りです。



No	回線	接続機器	バージョン	注意喚起	調査結果
1	CAF00001	A社 Router-01	調査不可 (IDPASS不明のため)	–	最新バージョン：x.x.x 稼働中のファームウェアバージョンを確認し、必要に応じてアップデートをご検討ください。
2	CAF00002	B社 Router-02	調査不可 (IDPASS不明のため)	–	公開情報がないため、ベンダーに問合せし、稼働中のファームウェアバージョンが最新でない場合、必要に応じてアップデートをご検討ください。
3	CAF00003	C社 Router-03	xx.xx.xx	注意	OSPFプロトコルに関する脆弱性で、内部犯によるルーティングテーブル改ざん、DoS攻撃の可能性があるため、ファームウェア最新版(xx.xx.xx)へのアップデートをご検討ください。
4	CAF00004	A社 Router-01	調査不可 (IDPASS不明のため)	–	最新バージョン：x.x.x 稼働中のファームウェアバージョンを確認し、必要に応じてアップデートをご検討ください。
5	CAF00005	D社 Router-04	xx.xx.xx	注意	遠隔の第三者によって、サービス運用妨害(DoS) 攻撃を受ける可能性がありますので、ファームウェア最新版へのアップデートをご検討ください
6	CAF00006	D社 Router-04	調査不可 (IDPASS不明のため)	–	最新バージョン：xx.xx.xx 稼働中のファームウェアバージョンを確認し、必要に応じてアップデートをご検討ください。
7	CAF00007	A社 Router-01	調査不可 (IDPASS不明のため)	–	最新バージョン：x.x.x 稼働中のファームウェアバージョンを確認し、必要に応じてアップデートをご検討ください。

外部ネットワーク接続点　調査結果

外部ネットワーク接続点の見える化 <現地検出>

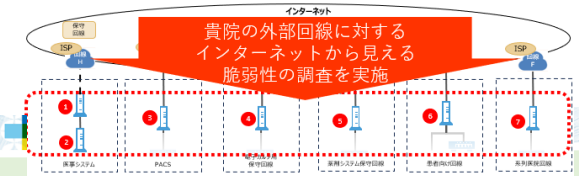
貴院の外部ネットワーク接続点を俯瞰的に見える化した結果は以下の通りです。
・現地で検出した回線終端装置の利用用途や電子カルテシステムとの接続があるか確認いただき、管理対象への追加をお願いします。

No	検出回線終端装置	設置場所	No	検出回線終端装置	設置場所
1	 CAF00008	2Fサーバ室 ラック	6		
2	 CAF00009	2Fサーバ室 ラック	7		
3	 CAF00010	1F診療室 机上	8		
4	 CAF00011	1F受付 机上	9		
5			10		

外部ネットワーク接続点　調査結果

外部ネットワーク接続点のセキュリティ対策状況（1/2）

貴院の外部ネットワーク接続点のネットワークに係るセキュリティ対策状況は以下の通りです。

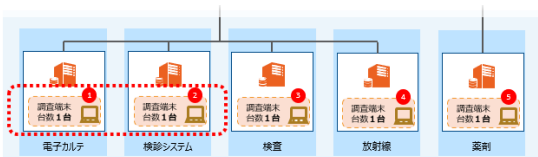


No	回線	注意喚起	応答ポート	調査結果
1	CAF00001	–	なし	オープンポートの取得ができませんでした。
2				
3	CAF00002	注意	500／udp	・リモートホストで Internet Key Exchange（IKE）の実行が有効になっているようです。 ・これは、通常は VPN サーバーを示します。VPN サーバーは、リモートホストを内部リソースに接続するために使用されます。 この VPN エンドポイントの使用が、所属する組織のセキュリティポリシーに則って実行されていることを確認してください。 ・オープンポートに紐づく脆弱性は検出されませんでした。
4	CAF00003	–	なし	オープンポートの取得ができませんでした。
5	CAF00004	–	–	閉域網のため脆弱性診断を実施していません。
6	CAF00005	–	なし	オープンポートの取得ができませんでした。
7	CAF00006	–	–	閉域網のため脆弱性診断を実施していません。

外部ネットワーク接続点　調査結果

ランサムウェア感染への備え（1/3）

端末でのランサムウェア感染への対応状況調査結果は以下の通りです。



端末①：HOSTNAME-01				
Windows OSバージョン	Windows10 Pro 21H2 xxxxx.xxxx	サポート状況		なし
Windows Update適用状況	3ヶ月以内の適用なし	USB使用制限 (端末設定)		なし
インターネット接続	なし	外部接続点 (デフォルトゲートウェイ)		–
ウィルス対策ソフト インストール有無	あり	ソフト名	No.1	Trend Micro Apex One
			No.2	–
備考	・サポート終了したWindowsを利用中のため、セキュリティパッチ等が提供されない可能性があります。Windowsのアップグレードを検討してください。 ・端末設定では、USB制御を実施していないようです。セキュリティ製品でUSB制御を実施している場合もあるので、端末管理者に確認をお願いします。			

端末②：HOSTNAME-02				
Windows OSバージョン	Windows10 Pro 20H2 xxxxx.xxxx	サポート状況		なし
Windows Update適用状況	3ヶ月以内の適用なし	USB使用制限 (端末設定)		なし
インターネット接続	なし	外部接続点 (デフォルトゲートウェイ)		–
ウィルス対策ソフト インストール有無	あり	ソフト名	No.1	ESET Security
			No.2	–
備考	・サポート終了したWindowsを利用中のため、セキュリティパッチ等が提供されない可能性があります。Windowsのアップグレードを検討してください。 ・端末設定では、USB制御を実施していないようです。セキュリティ製品でUSB制御を実施している場合もあるので、端末管理者に確認をお願いします。			

オフラインバックアップの整備支援

オフラインバックアップの整備支援（全体像）

- **ランサムウェア対策において重要な対策手段となり得る「オフラインバックアップ」について、病院のバックアップ取得状況を適切に把握した上で、必要に応じてオフラインバックアップ計画書の策定、構築支援、構築後の継続的な運用・維持について、病院・電子カルテベンダーと協力しながら実施します。**

オフラインバックアップの構成に関する要件確認の支援

■医療機関の電子カルテバックアップ状況、オフラインバックアップ検討状況の把握
■本事業におけるオフラインバックアップの要件を医療機関へ展開、オフラインとみなせるか否かの確認を支援

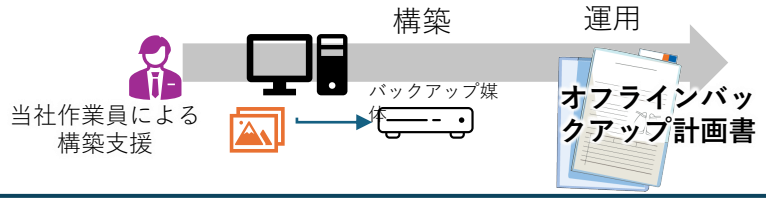
要件確認の結果、整備支援が必要な医療機関様へ追加で以下の支援を実施

オフラインバックアップ計画の策定支援

■オフラインバックアップ未実施病院の構築支援に向けた技術方式・実現方法、運用・維持の検討、計画書の作成

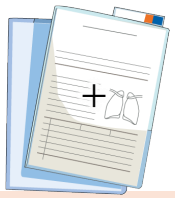
オフラインバックアップ環境の構築支援

■オフラインバックアップの実施に向けた現地構築支援作業



※必要な機器・サービスやそれらの調達にかかる費用、保守費用、電カルベンダーの設定費等は本事業の対象外。

オフラインバックアップ計画書



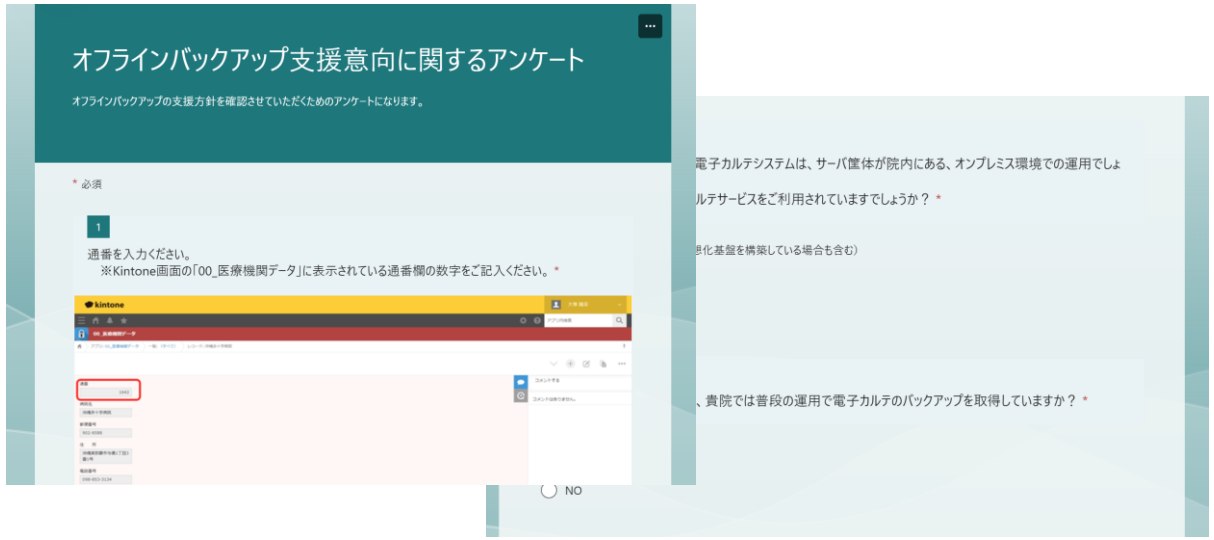
支援方針報告書

病院様へご報告

支援方針の決定

- 各医療機関様への支援方針を策定するため、「別紙5_各媒体におけるオフライン状態の定義」に記載の内容をご確認の上、「セキュリティ確保事業ポータル（以下、ポータルシステム）」経由で配布するWebアンケート（Microsoft Forms）へのご回答をお願いします。
- 電子カルテベンダ様等とオフラインバックアップの方針を検討中であり、且つ、本事業での支援が不要な医療機関様は、アンケートにてその旨ご回答ください。
- 既にオフラインバックアップを取得済の場合、アンケートにその旨ご回答ください（本事業での支援対象外となります）。

Webアンケートイメージ



Webアンケートの結果より、本事業における医療機関様への支援方針を決定

支援方針　※各方針の詳細は次ページに記載

支援A	支援B	支援C	報告のみ	対象外

支援方針ごとの対応範囲（支援A、支援B、支援Cの場合）

- **各支援方針において、医療機関様で対応が必要となる事項は下記のとおりとなります。**
- **既存バックアップのオフライン化を実現する媒体等の物品は、医療機関様にて調達いただく必要があります。**

支援ケースごとの対応範囲

支援方針	概要	医療機関様で必要な対応	本事業での支援対応
支援A 支援B	• 医療機関様にて、本事業にて支援可能なサーバ、物品を新設する意向あり**※1** • 【支援A】サーバ、物品の調達が年度内に可能 • 【支援B】サーバ、物品の調達は次年度以降	• Webアンケート回答 • 支援事業者との打ち合わせ対応（2~3回程度） • 新設サーバ、バックアップ媒体の調達 • 新設サーバ、バックアップ媒体の保守手配 • 既存機器（電子カルテサーバ、バックアップサーバ、NW機器等）の設定変更対応（手配） • 【支援Aのみ】現地作業における立ち合い対応 • 【支援Bのみ】新設サーバの構築作業（次年度以降）	• 本事業におけるオフラインバックアップの要件を医療機関様へ共有 • 打ち合わせにて医療機関様へ既存バックアップの状況、計画の意向を確認 • 医療機関様の意向をもとに、オフラインバックアップの計画・運用手順の策定を支援 • 【支援Aのみ】新設サーバ、バックアップ媒体の現地構築、設置対応 • 【支援Bのみ】新設サーバ、バックアップ媒体の現地構築手順を医療機関様へ提供
支援C	• 医療機関様にて支援可能なサーバを導入の意向なし • 既存設備に、本事業にて支援可能な媒体を接続**※2**	• Webアンケート回答 • 支援事業者との打ち合わせ対応（1回程度） • バックアップ媒体の調達 • バックアップ媒体の保守手配 • 既存機器（電子カルテサーバ、バックアップサーバ、NW機器等）の設定変更対応（手配）	• 本事業におけるオフラインバックアップの要件を医療機関様へ共有 • 打ち合わせにて医療機関様へ既存バックアップの状況、計画の意向を確認 • 医療機関様の意向をもとに、オフラインバックアップの計画の策定を支援

※1、※2・・・本事業で支援可能な物品は、「別紙6_オフラインバックアップ支援可能物品一覧」に記載の製品となります

支援方針ごとの対応範囲（対象外、報告のみの場合）

- **アンケートの回答より、対象外、報告のみのケースとなることが確認できた医療機関様においては、原則、アンケート回答以降に必要となる対応はございません。**

支援ケースごとの対応範囲

支援方針	概要	医療機関様で必要な対応	本事業での支援対応
報告のみ	• アンケートにて、電子カルテベンダ様等とオフラインバックアップの方針検討中であり、支援不要な旨回答を受領	• なし（Webアンケート回答のみで完了）	• 本事業におけるオフラインバックアップの要件を医療機関様へ共有 • 医療機関様で検討中のオフラインバックアップ方針（構成概要、導入予定時期）をヒアリングし、厚労省へ報告
対象外	• アンケートにて、既存環境ですでに電子カルテのオフラインバックアップの運用が開始している旨、回答を受領	• なし（Webアンケート回答のみで完了）	• 本事業におけるオフラインバックアップの要件を医療機関様へ共有 • 医療機関様で導入済のオフラインバックアップ方針（構成概要）をヒアリングし、厚労省へ報告

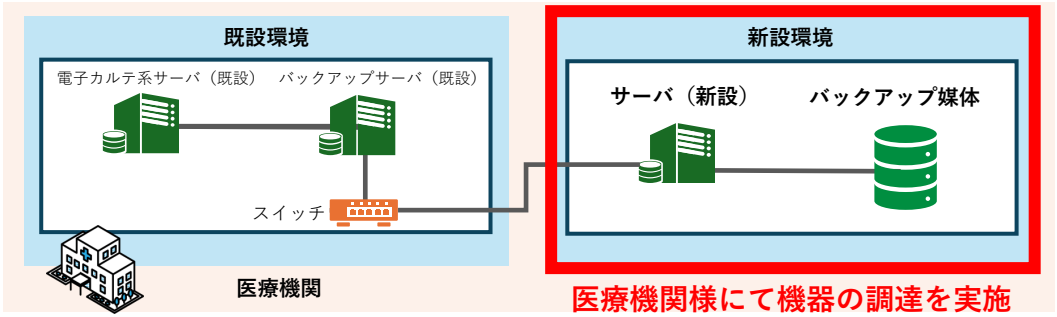
オフラインバックアップ構成

院内の物理媒体に保存の場合

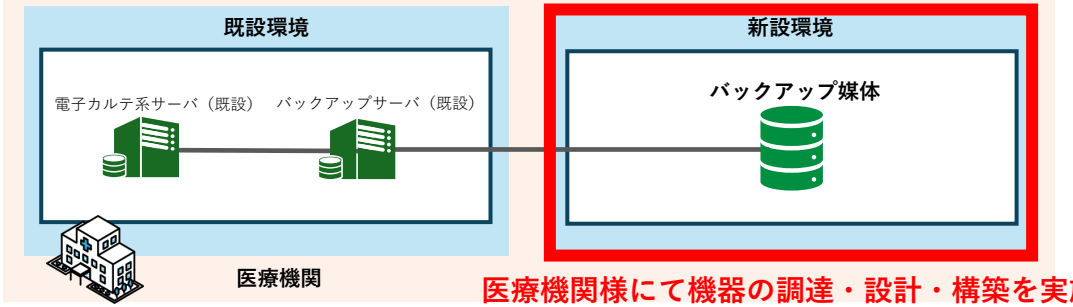
- 院内の物理媒体へオフラインバックアップを取得する構成を希望の医療機関様については、以下の構成にて支援を実施します。
  【支援A,B】　サーバを院内へ新設し、バックアップ媒体を接続する構成
  【支援C】　　既設環境にバックアップ媒体を接続する構成

- いずれの支援パターンにおいても、バックアップ媒体、および新設サーバは医療機関様にて購入、保守手配をご対応いただく前提となります。
- 既設環境から新設環境へバックアップデータを転送するための既存機器の設計、設定変更、ケーブル等のご用意は医療機関様にてご対応いただく前提となります。

構成パターン（支援A,Bの場合）



構成パターン（支援Cの場合）

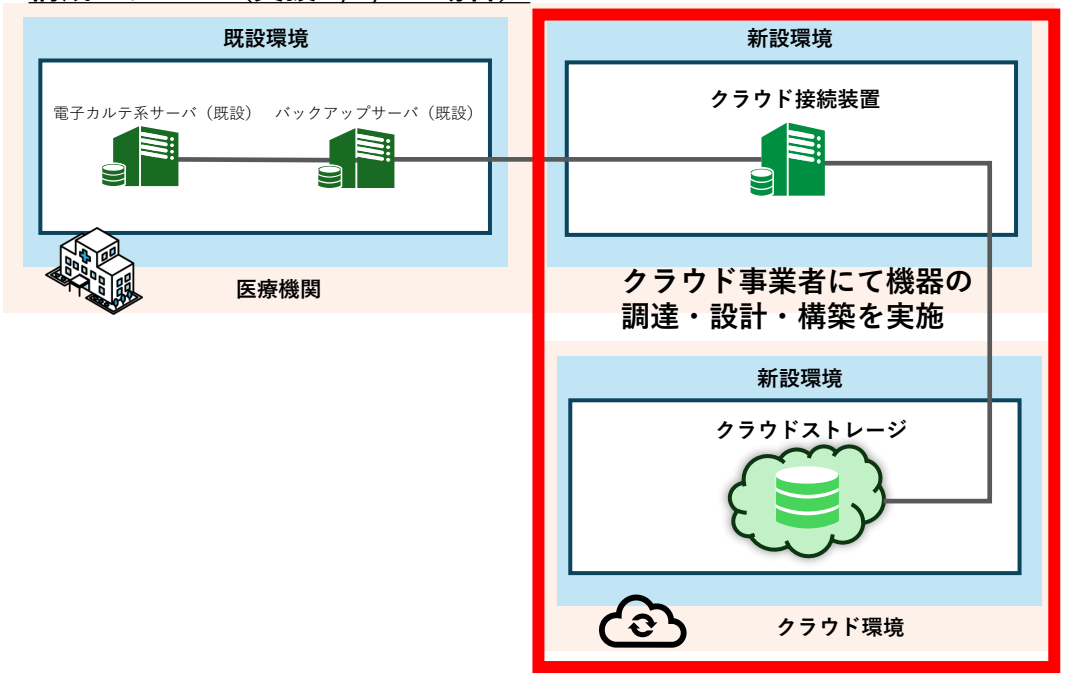


外部クラウド環境保存の場合

- 外部クラウド環境へオフラインバックアップを取得する構成を希望の医療機関様については、当社指定のクラウドサービスを用いた支援を実施します。
  【支援A,B,C】
  クラウド接続装置を院内へ新設し、クラウドストレージへ接続する構成
  ※サーバの新設は不要となります。

- いずれの支援パターンにおいても、クラウド接続装置はクラウド事業者にて調達・設置します。医療機関様でのご対応は不要となります。
- 既設環境から新設環境へバックアップデータを転送するための既存機器の設計、設定変更、ケーブル等のご用意は医療機関様にてご対応いただく前提となります。

構成パターン（支援A,B,Cの場合）



2. 実施フロー

実施項目一覧（1/2）

	No	項目	内容	期日/日程	対象	チェック欄
共通（事前準備）	1	**病院説明会への参加**	病院向け説明会へのご参加（本動画の視聴）をお願いします。病院内のご関係者様へ病院説明会の内容のご共有をお願いします。	7/3（本日）	全医療機関	□
	2	**テストメールへの返信**	事務局よりテストメール受信後、事務局宛にご返信をお願いします。	メール受信後 3日以内	全医療機関	□
	3	**提出関連資料の確認**	前項２．の「テストメール」にご返信頂いた後、事務局より「提出関連資料一式」が届きますので、内容のご確認をお願いします。	メール到着次第	全医療機関	□
	4	**ポータルシステムへのログイン**	前項３．とともに「ポータルシステム利用に関するご案内」（利用手順、ログイン情報）が届きます。ご案内に従ってポータルシステムへアクセスいただき、基本情報に誤りがないかご確認をお願いします。	メール到着後 3日以内	全医療機関	□
外部ネットワーク接続の俯瞰的把握、安全性の検証・調査	1	**提出資料の準備**	「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認の上、「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」、関連資料を事務局へご提出をお願いします。	9/30まで 早期提出推奨	全医療機関	□
	2	**情報収集**	「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の記入にあたって、外部接続回線の洗い出し、調査端末（PC）の選定、グローバルIPアドレスの確認をお願いします。	ー	全医療機関	□
	3	**関係者へのご確認**	前項２．の「情報収集」にあたって、病院内のご関係者様や関連ベンダへのご確認をお願いします。特に、調査対象機器のログイン情報は当日必要となるため予めご用意をお願いします。	ー	全医療機関	□
	4	**現地調査日の調整**	必要資料を提出いただいた後、事務局より順次日程調整のご連絡をします。	資料提出後順次	全医療機関	□
	5	**脆弱性診断日の調整**	現地調査日から1週間～1か月程度を目途に対象回線に対して脆弱性診断を遠隔で実施します。脆弱性診断の実施日が確定しましたら、事務局よりご連絡します。	資料提出後順次	全医療機関	□
	6	**現地調査時の立会い**	現地調査時の立会いをお願いします。調査対象機器が設置されている部屋へのご案内、調査対象端末へのログインをお願いします。事前にログイン用IDパスワードの準備をお願いします。	現地調査当日	全医療機関	□
	7	**グローバルIPアドレスの確認**	脆弱性診断の実施対象のグローバルIPアドレスの最終確認を行うため、事務局へご連絡をお願いします。	脆弱性診断当日	一部医療機関（動的IPアドレスが対象の場合のみ）	□
	8	**調査報告書の受領**	事務局より調査結果をまとめた調査報告書をポータルシステムへアップロードします。	調査後 約１.5か月後	全医療機関	□

実施項目一覧（2/2）

	No	項目	内容	期日/日程	対象	チェック欄
オフラインバックアップ	1	**アンケート回答**	「オフラインバックアップ支援意向に関するアンケート」（Microsoft Forms）へのご回答をお願いします。 アンケートにご回答するにあたり、「別紙5_各媒体におけるオフライン状態の定義」、「別紙6_オフラインバックアップ支援可能物品一覧」を参照の上、現在の電子カルテのバックアップ方法等の詳細について、ご確認をお願いします。	7/31まで	全医療機関	□
	2	**打合せ**	アンケートの回答内容をもとに、打合せが必要な場合は、事務局より日程のご調整をさせていただきます。 WEB会議（Microsoft Teams）のURLを事務局よりメールにてご案内します。	ー	一部医療機関 （支援A～Cの医療機関※）	□
	3	**機器調達**	本事業で新たにオフラインバックアップの構築を実施する場合、必要機器の調達をお願いします。	構築日まで	一部医療機関 （支援Aの医療機関※）	□
	4	**現地訪問日の調整**	本事業で構築支援を行う場合、事務局より現地訪問日の調整のご連絡をします。	順次	一部医療機関 （支援Aの医療機関※）	□
	5	**現地訪問時の立会い**	現地訪問時の立会いをお願いします。構築対象機器が設置されている部屋へのご案内をお願いします。	現地訪問当日	一部医療機関 （支援Aの医療機関※）	□
	6	**オフラインバックアップ計画書の受領**	事務局より調査結果をまとめた「オフラインバックアップ計画書」をポータルシステムへアップロードしますので、ご確認をお願いします。	実施後 約1か月後	一部医療機関 （支援A～Cの医療機関※）	□

※オフラインバックアップの支援に関するパターンはP13,14参照

実施フロー

共通(事前準備)

【共通の流れ】

1 **病院説明会への参加**　本日（7/3）

病院向け説明会へのご参加（本動画の視聴）をお願いします。

必要に応じて病院内のご関係者様※へ病院説明会の内容をご共有いただけます。質問がある場合には、事務局宛にご連絡をお願いします。（事務局連絡先はP53参照）

※本事業は、電子カルテに接続する基幹系ネットワークのセキュリティ調査、及び電子カルテのバックアップに関する事業のため、電子カルテ・部門システム等を管理されている方、協力ベンダー　など

2 **テストメールへの返信**　7/3～7/6頃まで順次

事務局より、事前に都道府県にご報告頂いている病院担当者宛に**テストメールが7/3～7/6頃までに順次届きます。**

テストメール受信後、**3日以内に事務局宛にご返信をお願いします。**
※以降のやり取りはテストメールへご返信いただいた担当者宛にご連絡いたします。

テストメールイメージ

送信者	サイバーセキュリティ確保事業 事務局(pj-mhlw-gm@east.ntt.co.jp)
件名	NTT東日本より　メールアドレスのご確認(厚生労働省様サイバーセキュリティ確保支援事業)

●●病院
▲▲課
■■様

平素より大変お世話になっております。
NTT東日本でございます。
この度、厚生労働省様によるサイバーセキュリティ確保事業について、ご支援申し上げます。

本メールは、メールアドレスをご確認させていただくためのテストメールです。
このメールに対してご返信いただけますよう、よろしくお願いいたします。

ご返信をいただけましたら、
このメールアドレスあてに、今後のご支援に必要なファイルをメール添付にてお送りいたします。

よろしくお願いいたします。

****
サイバーセキュリティ確保支援事業　事務局
東日本電信電話株式会社
ITOビジネス推進部　ITOコーディネート部門
第一サポート担当
●●　▲▲

〒XXX-XXXX　XXXXXXX
TEL：03-6915-4268
Mail（共通）：pj-mhlw-gm@east.ntt.co.jp
****

実施フロー

共通(事前準備)

【共通の流れ】

3 **提出関連資料の確認**　テストメール受信後、順次

上記２．の「テストメール」にご返信頂いた後、**事務局より「提出関連資料一式」が届きますので、内容のご確認をお願いします。**
同様の資料は、ポータルシステムへも掲載予定です。

4 **ポータルシステムへのログイン**　ご案内到着後～３日以内

上記３．の関連資料とともに、**「ポータルシステム利用に関するご案内」（利用手順、ログイン情報）が届きます。**

ご案内に従ってポータルシステムへアクセスいただき、**基本情報に誤りがないかご確認をお願いします。**
ご確認いただいた後、チェックボックスへのチェックをお願いします。
記載情報に誤りがあった場合は、**３日以内にポータルシステム内の備考欄へ記載をお願いします。**

お早めのアクセスのご協力をお願いします

ここまでが共通の流れです。
次ページより、「ネットワーク調査」の流れをご説明します。

メールイメージ

＜件名＞NTT東日本より　サイバーセキュリティ確保支援事業　ご支援開始にあたってのご案内

＜メール本文＞
平素より大変お世話になっております。
NTT東日本でございます。
テストメールへご返信いただき、ありがとうございました。

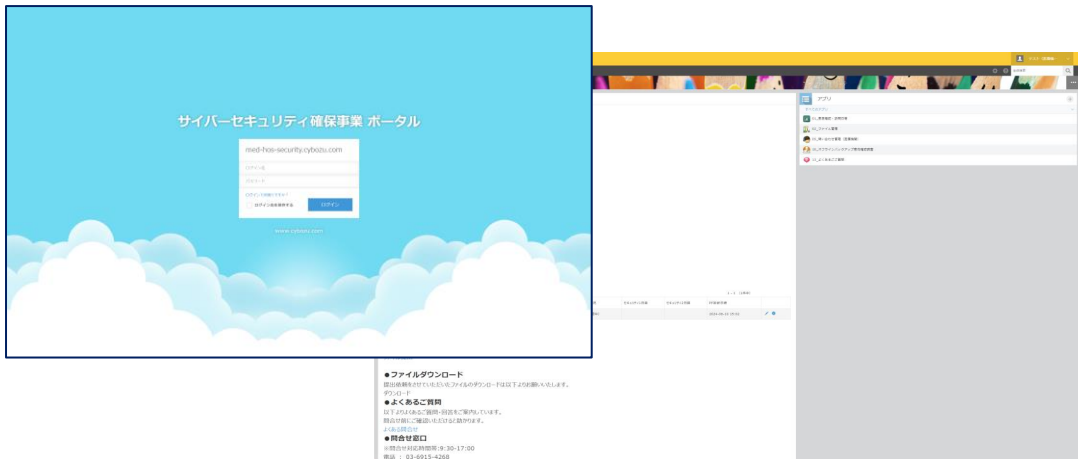
この度、厚生労働省様によるサイバーセキュリティ確保事業について、
ご支援申し上げることになりました。よろしくお願いいたします。
早速ではございますが、ご支援を始めるにあたり、以下のファイルをお送りいたします。

・ポータルシステムご利用開始のためのご案内
・セキュリティ現地調査のために事前にご提出いただく様式のご案内

添付ファイルをご確認いただき、以下の順でご対応をお願いいたします。
①ポータルシステムの開通のご対応（電子証明書のインストール、ログイン）
②事前にご提出いただく様式の記入、資料のご用意
③ポータルシステムへ、様式、資料のアップロード

ご支援のやりとりは、履歴として見える形で残すことにより対応漏れを無くすため、
基本的には、ポータルシステム上のチャット機能で行わせていただければと存じます。
まずはポータルシステムの利用開始準備をお願いいたします。

ポータルシステムの利用でご不明な点があれば、メールまたはお電話でお問い合わせください。
よろしくお願いいたします。



実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～事前～】

1　提出資料の準備　9/30※まで提出

1）医療機関記入依頼書（回線・機器情報等記入）

「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認の上、「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」のご記入、事務局へご提出をお願いします。

2）その他必要書類

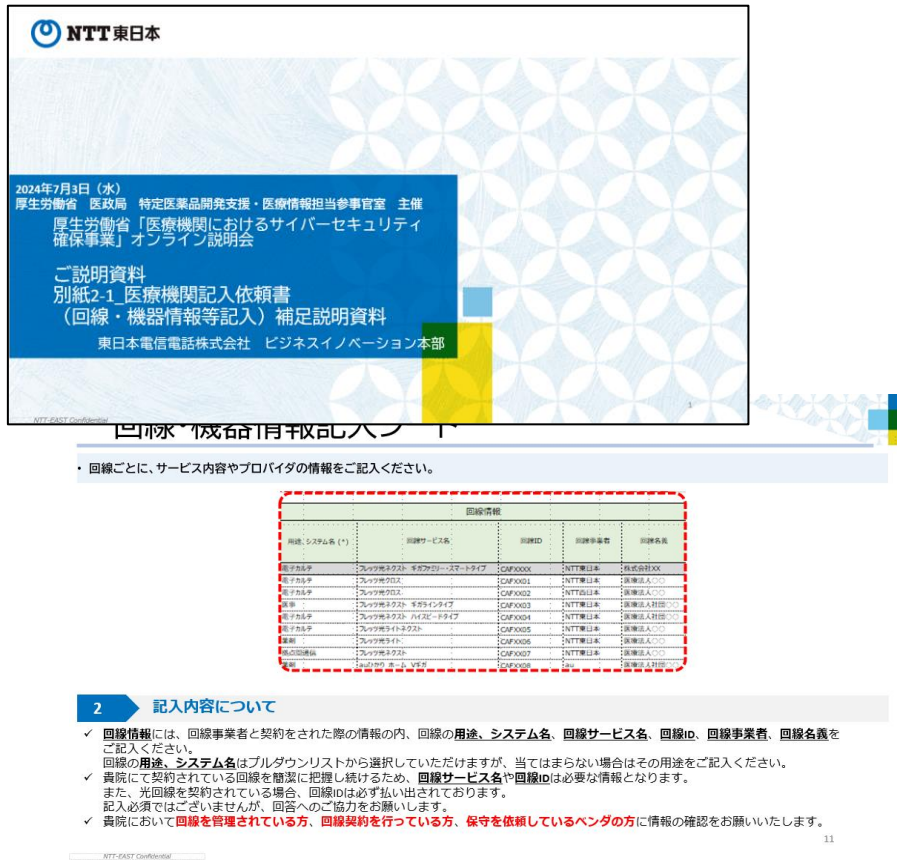
以下の書類のご準備と事務局へのご提出をお願いします。（詳細はP46参照）

【必須】※「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の設置場所記入シートに添付
- 平面図
- フロア図

【任意】
- ネットワーク概要図

※必要資料をご提出いただいた順に、順次事務局より日程調整を行います。
1）～7月17日にご提出の場合→最短8月22日より現地調査を実施
2）～8月17日にご提出の場合→最短9月22日より現地調査を実施
3）～9月17日にご提出の場合→最短10月22日より現地調査を実施
※必要書類の早期提出にご協力願います。

別紙2-2_医療機関記入依頼書(回線・機器情報等記入)補足説明資料



実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～事前～】

2　情報収集

1）外部接続点（外部接続回線）の洗い出し

「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の
記入にあたって、
電子カルテネットワークに接続されている回線※・ネットワーク機器情報及び回線終端装置（ONU）の設置場所等のご確認をお願いします。
※ベンダーが院内に設置している保守用回線も含みます。

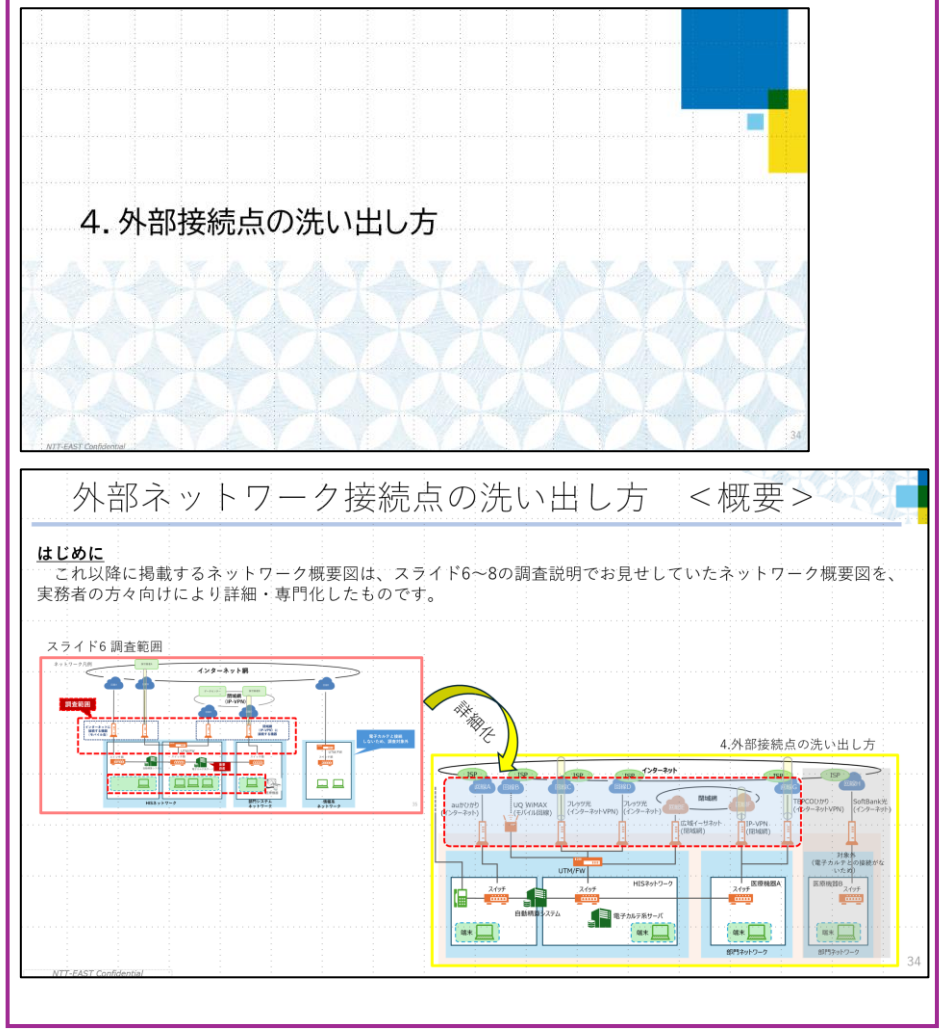
具体的な対象範囲や確認方法については、本資料のP33～をご確認下さい。

2）調査端末（PC）の選定

「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の
記入にあたって、
セキュリティ対策状況を確認したい**PC端末を5台選定をお願いします。**

電子カルテシステムとの接続がある端末を選定してください。電子カルテ端末から1台、その他、主要な部門システムから1台ずつの選定を推奨します。

外部接続点の洗い出し方　本資料P33～



実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～事前～】

2　情報収集

3）グローバルIPアドレスの事前確認

「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の
記入にあたって、
脆弱性診断対象機器のグローバルIPアドレスの確認をお願いします。

具体的な確認方法については、
「別紙4_ベンダ様向け脆弱性診断説明資料」をご確認下さい。

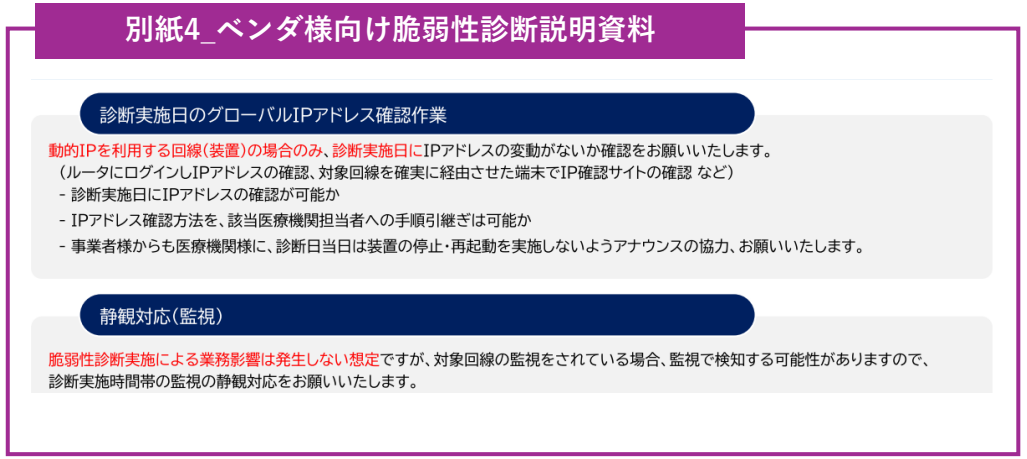
3　関係者へのご確認　**現地調査前／脆弱性診断前まで**

前項の必要情報を収集するにあたっては、**病院内のご関係者様や関連ベンダへのご確認をお願いします。**

特に、調査対象機器のログイン情報は当日必要となるため予めご用意をお願いします。

本事業は、より正確な情報を事前に収集いただくことで、より精度の高い調査となりますので、お手数ですがご協力をお願いします。

別紙4_ベンダ様向け脆弱性診断説明資料



診断実施日のグローバルIPアドレス確認作業

動的IPを利用する回線(装置)の場合のみ、診断実施日にIPアドレスの変動がないか確認をお願いいたします。
（ルータにログインしIPアドレスの確認、対象回線を確実に経由させた端末でIP確認サイトの確認 など）
- 診断実施日にIPアドレスの確認が可能か
- IPアドレス確認方法を、該当医療機関担当者への手順引継ぎは可能か
- 事業者様からも医療機関様に、診断日当日は装置の停止・再起動を実施しないようアナウンスの協力、お願いいたします。

静観対応(監視)

脆弱性診断実施による業務影響は発生しない想定ですが、対象回線の監視をされている場合、監視で検知する可能性がありますので、
診断実施時間帯の監視の静観対応をお願いいたします。

実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～事前～】

4 現地調査日の調整

資料提出確認後順次

必要資料をご提出いただき、事務局で事前資料の準備が完了と確認できた場合に、順次日程調整のご連絡をします。

日程確定後、変更を希望される場合は、**現地調査日の10日前に事務局へご連絡をお願いします。**
直前の日程変更は、期間内に調査を実施できない可能性があるため、ご協力よろしくお願いします。

5 脆弱性診断日の調整

現地調査日から1週間～１か月程度※を目途に対象回線に対して脆弱性診断を遠隔で実施します。（病院への訪問はございません）
※調査時期は多少前後する可能性あります。

脆弱性診断の実施日が確定しましたら、事務局よりご連絡します。

対象回線の監視をされている場合、監視検知する可能性があるため、必要に応じて、監視の静観対応をお願いします。**事前に病院内のご関係者様、及び診断対象回線の保守ベンダへ予め連絡・周知をお願いします。**
（詳細は「別紙4_ベンダ様向け脆弱性診断説明資料」をご確認ください）

別紙4_ベンダ様向け脆弱性診断説明資料

診断実施日のグローバルIPアドレス確認作業

動的IPを利用する回線(装置)の場合のみ、診断実施日にIPアドレスの変動がないか確認をお願いいたします。
（ルータにログインしIPアドレスの確認、対象回線を確実に経由させた端末でIP確認サイトの確認 など）
- 診断実施日にIPアドレスの確認が可能か
- IPアドレス確認方法を、該当医療機関担当者への手順引継ぎは可能か
- 事業者様からも医療機関様に、診断日当日は装置の停止・再起動を実施しないようアナウンスの協力、お願いいたします。

静観対応(監視)

脆弱性診断実施による業務影響は発生しない想定ですが、対象回線の監視をされている場合、監視で検知する可能性がありますので、診断実施時間帯の監視の静観対応をお願いいたします。

実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～事前～】

6 現地調査時の立会い

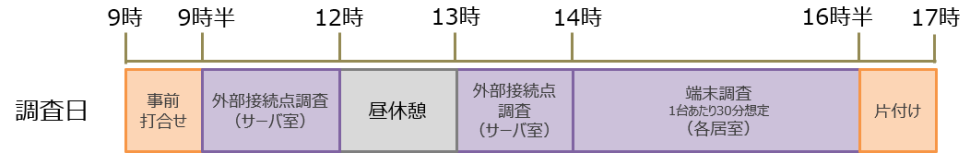
現地調査当日

現地調査時の立会いをお願いします。調査対象機器が設置されている部屋へのご案内、調査対象端末へのログインをお願いします。
また、作業員による調査対象端末の操作の許可※をお願いします。

※調査時に電子カルテ端末や部門システム端末の操作を行うため、当日作業員が操作できるよう関係者とのご調整を願いします。

当日スケジュール例※

調査日	時間帯	作業内容
1日目 2日目	午前	9:00 入館 9:00-9:30 作業前打合せ：作業計画の説明、設置場所確認、作業の流れ 9:30-12:00 外部接続点調査 調査対象の回線終端装置(ONU)の位置確認、各回線下部の接続構成確認、機器情報取得、写真撮影 調査対象のNW機器(ルータ・UTM)への接続調査ファームウェアバージョン確認
	午後	13:00-14:00 外部接続点調査 14:00-16:30 端末調査：事前に申告いただいた端末5台に対する調査 16:30-17:00 片付け・退館



※調査対象回線数・機器によって調査日数・作業時間は前後します。

7 グローバルIPアドレスの確認

脆弱性診断当日

脆弱性診断対象のグローバルIPアドレス（動的IPアドレスのみ）の最終確認を行っていただき、
「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」に記入したうえで
ポータルシステムにアップロードをお願いします。

具体的な確認方法については、「別紙4_ベンダ様向け脆弱性診断説明資料」 をご確認下さい。

実施フロー

ネットワーク調査

【外部ネットワーク接続の俯瞰的把握、安全性の検証・調査　～実施後～】

8 **調査報告書の受領**　**実施後1.5か月後目途**

事務局より調査結果をまとめた調査報告書をポータルシステムへ
アップロードしますので、ご確認をお願いします。

次ページより、「オフラインバックアップ」の流れをご説明します。

調査報告書　イメージ

実施フロー

オフラインバックアップ

【オフラインバックアップの流れ～事前～】

1　アンケート回答　**ポータルシステム利用開始～7/31まで**

ポータルシステムから、「オフラインバックアップ支援意向に関する
アンケート」（Microsoft Forms）へのご回答をお願いします。

アンケートにご回答するにあたり、現在の電子カルテのバックアップ方法等の
詳細について、ご確認をお願いします。

2　（必要に応じて）打合せ

アンケートの回答内容をもとに、打合せが必要な場合には、事務局よりご調整
のご連絡をさせていただきます※1。

事務局よりWEB会議※2をご案内しますので、当日はそちらのURLよりご参加
ください。

※1）電子カルテベンダーも打合せに参加頂くようご調整をお願いします。
※2）WEB会議はMicrosoft Teamsで行います。

Webアンケート　画面イメージ

実施フロー

【オフラインバックアップの流れ～事前～】

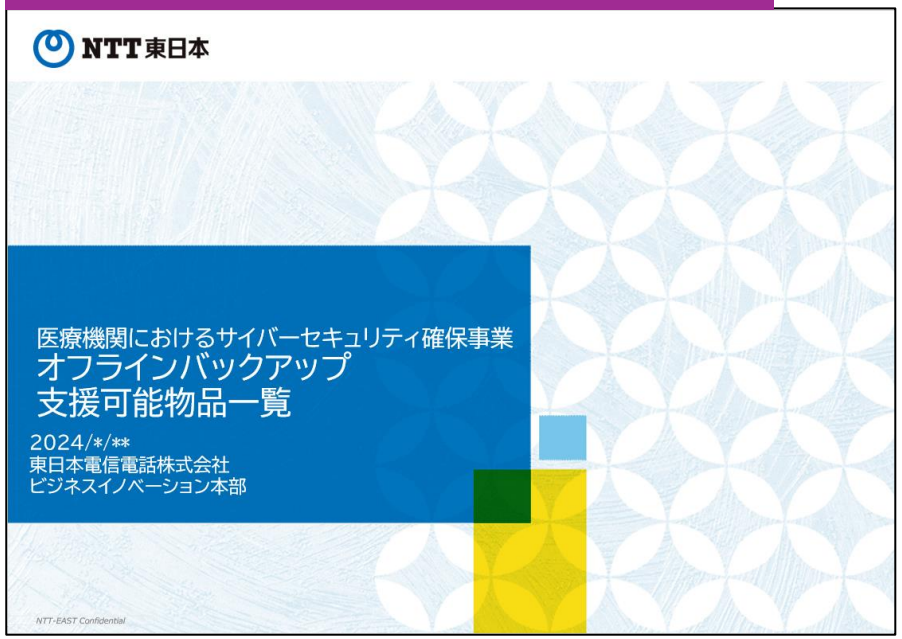
支援Aの場合（本事業で構築支援を実施する場合）

3　機器調達　構築当日まで

本事業で新たにオフラインバックアップの構築を実施する場合、必要機器※の調達をお願いします。

※必要な機器・サービスやそれらの調達、 保守手配、電子カルテベンダーの設定作業等の支援は本事業に含まれておりません。
※構築対象機器一覧は「別紙6_オフラインバックアップ支援可能物品一覧」をご確認ください。

別紙6_オフラインバックアップ支援可能物品一覧



支援Aの場合（本事業で構築支援を実施する場合）

4　現地訪問日の調整

本事業で構築支援を行う場合、事務局より現地訪問日の調整のご連絡をします。

日程確定後、変更を希望される場合は、**現地訪問日の7日前までに事務局へご連絡をお願いします。**
直前の日程変更は、期間内に構築支援を実施できない可能性があるため、ご協力よろしくお願いします。

実施フロー

【オフラインバックアップの流れ～当日・実施後～】

支援Aの場合（本事業で構築支援を実施する場合）

5 **現地訪問時の立会い** **現地訪問当日**

現地訪問時の立会いをお願いします。構築対象機器が設置されている部屋へのご案内をお願いします。

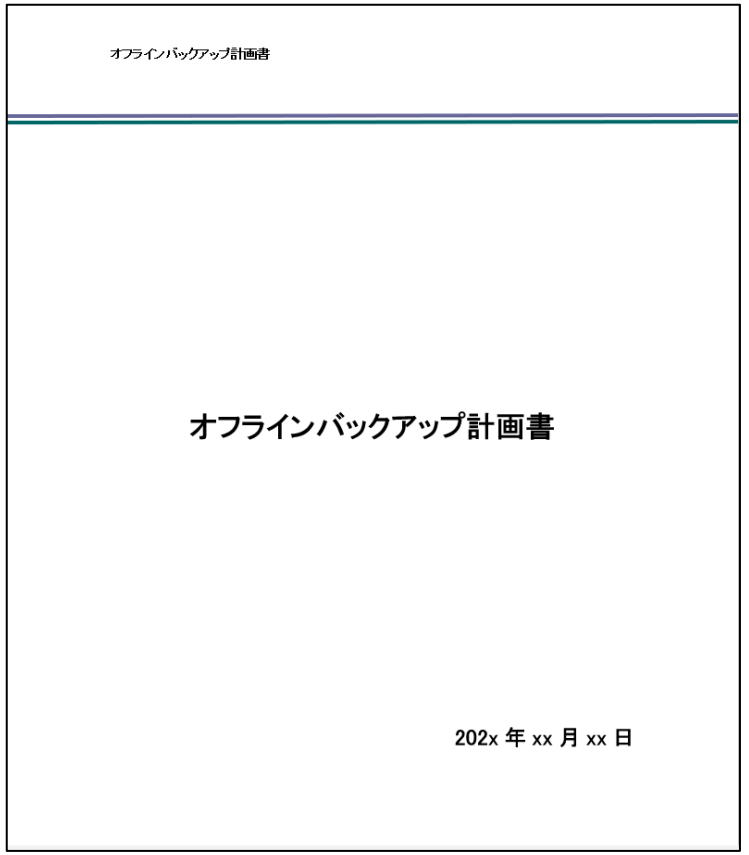
また、作業員による対象端末の操作の許可をお願いします。

支援A～Cの場合

6 **オフラインバックアップ計画書の受領** **実施後1か月後目途**

事務局より調査結果をまとめた「オフラインバックアップ計画書」をポータルシステムへアップロードしますので、ご確認をお願いします。

「オフラインバックアップ計画書」　イメージ


オフラインバックアップ計画書

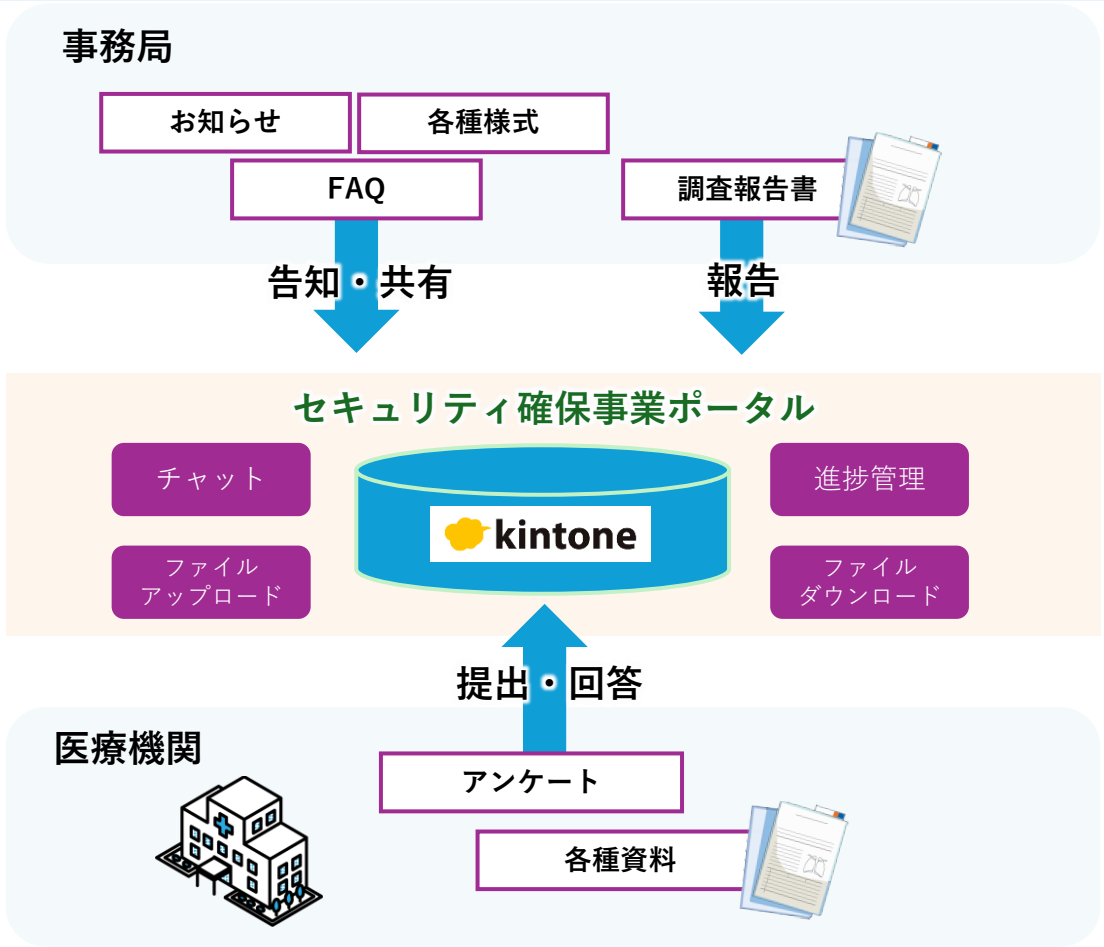
オフラインバックアップ計画書

202x 年 xx 月 xx 日

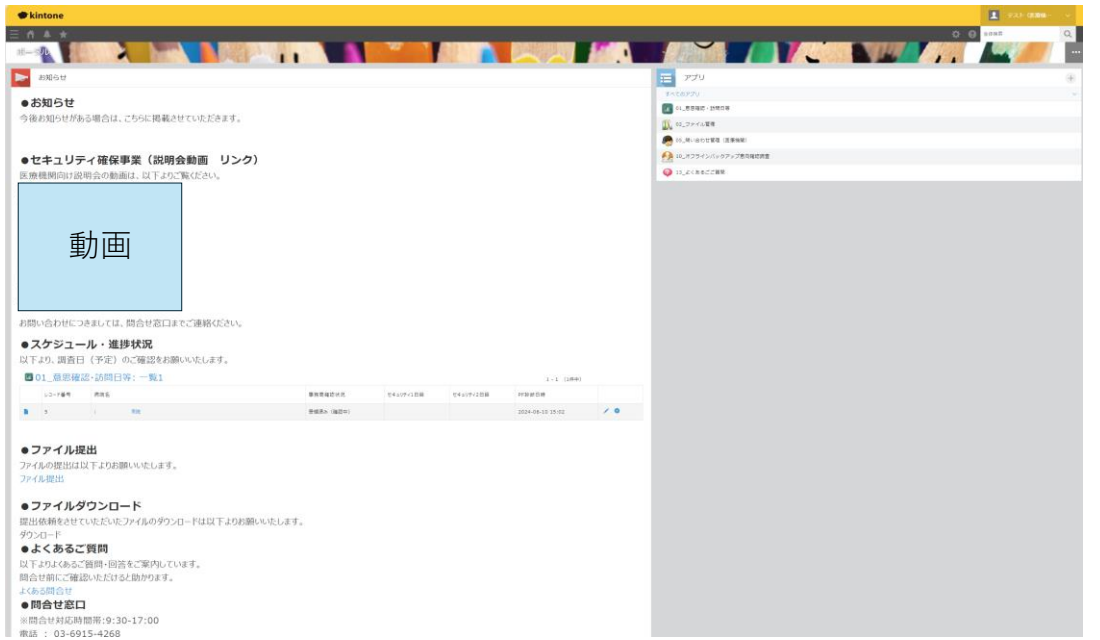
3. ポータルシステムについて

「セキュリティ確保事業ポータル」について

- **本事業に関するお知らせや周知事項、情報のやり取りを効率化するためにKintone（キントーン）を利用したポータルサイト「セキュリティ確保事業ポータル」を作成します。**
- **主に医療機関様へのお知らせの掲載や、事務局への資料の提出や報告書等のダウンロードにご利用いただきます。（利用方法の詳細は、別途送付する「ポータルサイト 設定マニュアル」をご確認ください）**



画面イメージ



（出典）kintone（キントーン）とは - サイボウズ (cybozu.co.jp)

利用開始の流れ

- **各医療機関様宛にメールにて、事前設定に必要な情報を送付いたします。**
- **メールを受領後、メールに記載のある手順に従い、設定いただき、以下のようにアクセスできるかをご確認お願いします。**
- **アクセスができない等の不具合や不明点は、事務局窓口までご連絡をお願いいたします。**

＜流れ＞

1. 当社にてシステムにお客様情報を登録
2. 当社のシステム上より医療機関にメールを送付
3. 各医療機関様にて事前設定
（①クライアント証明書をインストール）
4. 上記③の事前設定のうえ、
ブラウザより右記のログインURLにアクセス
メールにて送付したID・パスワードでログイン。
5. ※初回ログイン時のみ
“パスワードを変更してください”画面が表示されます。
ご自身で新しいパスワードを設定ください。
6. kintone を押下してください。
7. TOP画面が表示されます。

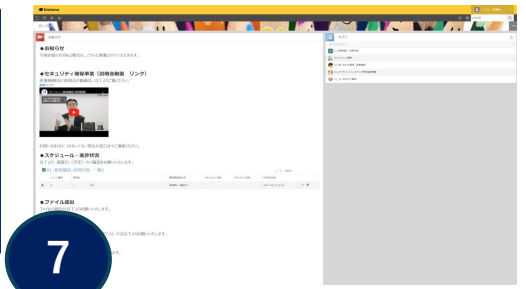
準備完了

メールの文面例や詳細な手順は、別途送付する「ポータルサイト 設定マニュアル」をご確認ください

ログインURL
https://med-hos-security.s.cybozu.com/

5

7



6

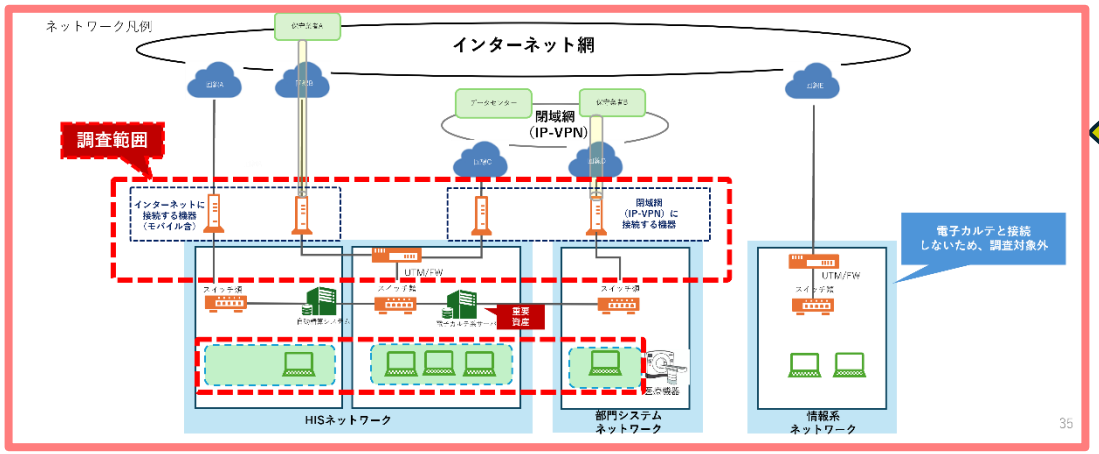
4. 外部接続点の洗い出し方

外部ネットワーク接続点の洗い出し方　＜概要＞

はじめに

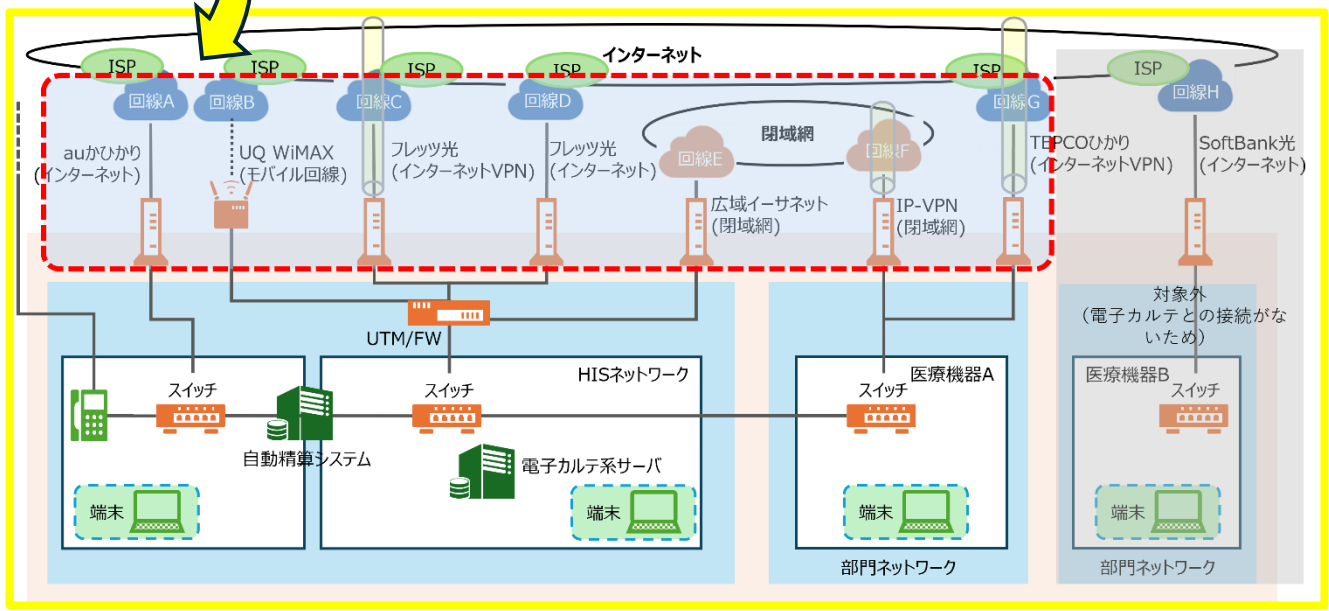
　これ以降に掲載するネットワーク概要図は、スライド6～8の調査説明でお見せしていたネットワーク概要図を、実務者の方々向けにより詳細・専門化したものです。

スライド6 調査範囲



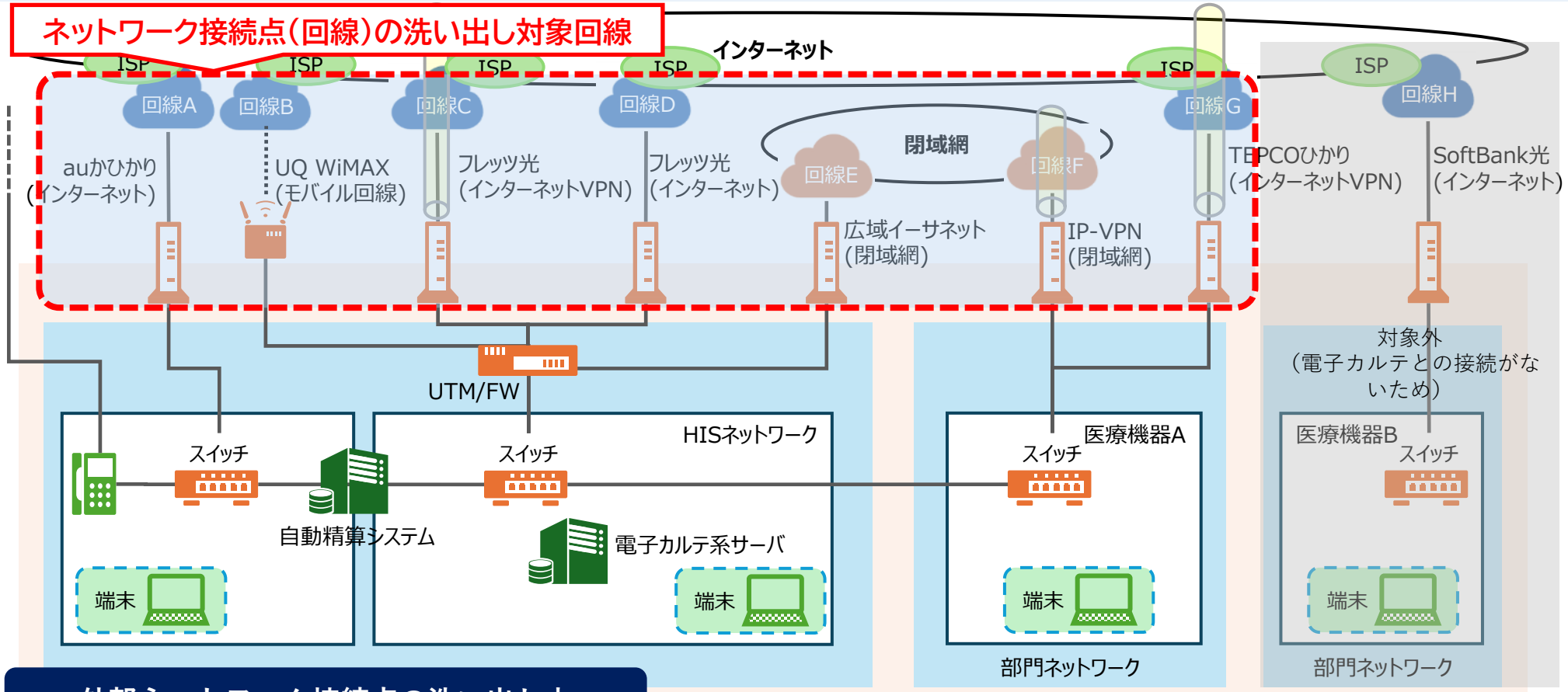
詳細化

4.外部接続点の洗い出し方



外部ネットワーク接続点の洗い出し方　＜概要＞

- **病院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、安全性の検証・調査を実施します。**
- **外部ネットワーク接続点を把握するため、電子カルテシステムに接続する回線のリストアップをお願いいたします。**



外部ネットワーク接続点の洗い出し方

- 外部ネットワーク接続点を洗い出すために実施いただきたい作業をまとめました。
- 次スライド以降の<STEP1>～<STEP7>の作業を実施してください。

外部ネットワーク接続点の洗い出し方　<流れ>

STEP 1

外部ネットワーク接続点(回線)の適用範囲の把握

電子カルテシステムに接続する回線の適用範囲を把握する

STEP 2

回線一覧管理台帳からのリストアップ

既に管理されている台帳から対象回線を確認する

STEP 3

各部門への問合せによる独自契約回線のリストアップ

部門毎に独自に準備した回線がないか確認する

STEP 4

各部門への問合せによる契約ベンダーのリストアップ

どこのベンダーと契約をしているか部門に確認する

STEP 5

契約ベンダーへの問い合わせによる回線のリストアップ

医療機関名義以外の回線がないかベンダーに確認する

STEP 6

目視確認によるリストアップ

収集した回線以外に引き込まれている回線がないか確認する

STEP 7

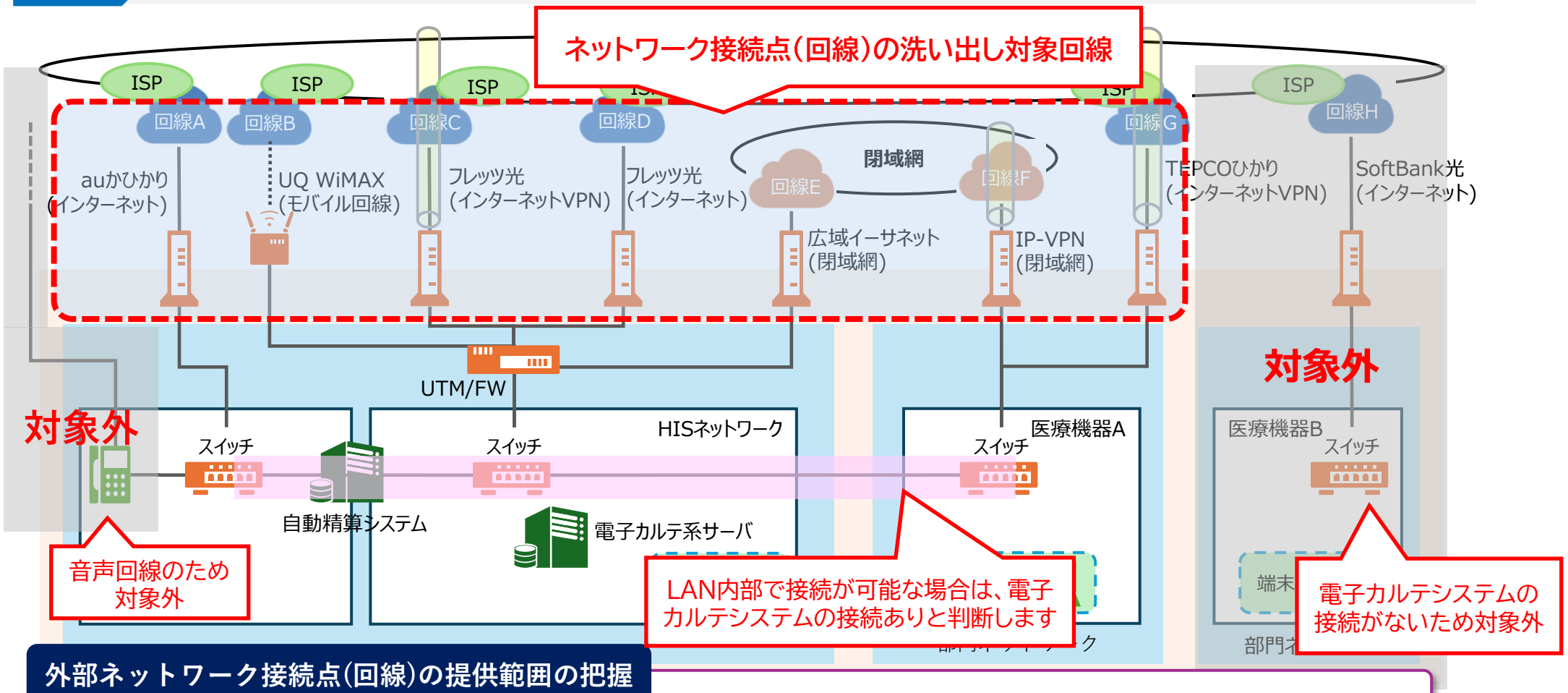
回線・機器情報記入シートへの記入

リストアップした回線情報の記入をお願いします。

※詳細は「別紙2-2_医療機関情報記入依頼（回線・機器情報等記入）補足説明資料」参照

外部ネットワーク接続点の洗い出し方　<STEP1>

1　外部ネットワーク接続点(回線)の提供範囲の把握

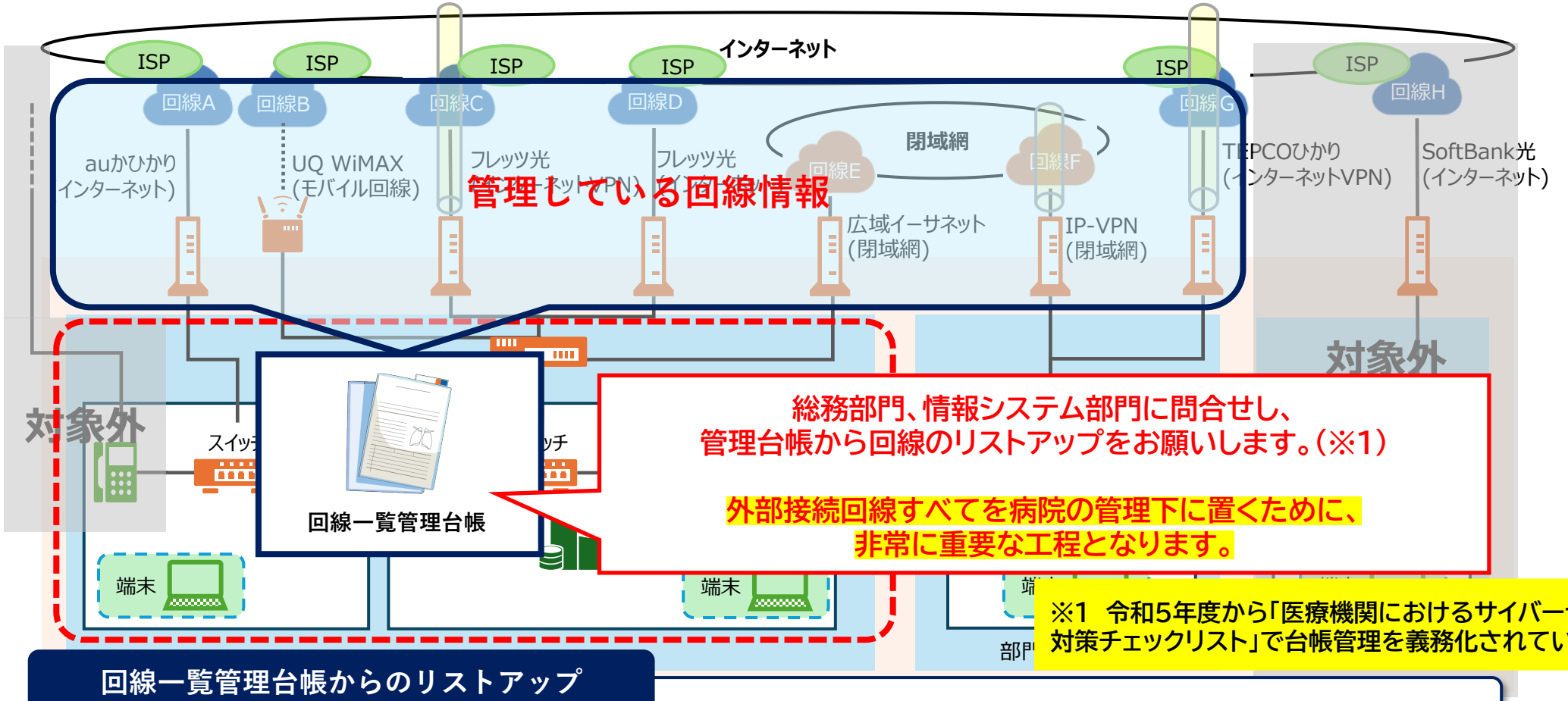


外部ネットワーク接続点(回線)の提供範囲の把握

- 電子カルテシステムに接続するすべての回線（有線、無線、回線業者不問）が対象となります。
- データ利用している回線を対象とし、音声回線は対象外とします。

外部ネットワーク接続点の洗い出し方　<STEP2>

2　回線一覧管理台帳からのリストアップ

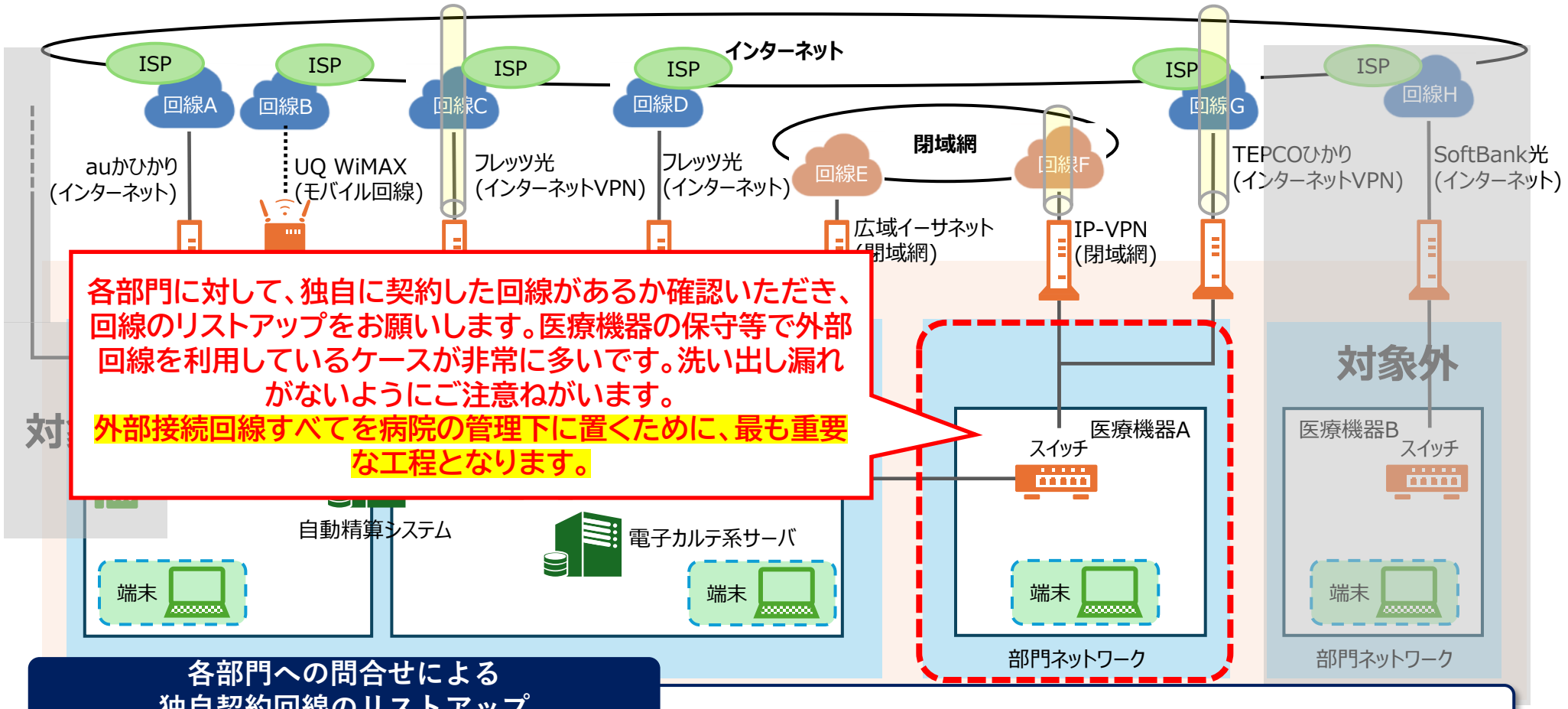


回線一覧管理台帳からのリストアップ

- 回線情報が管理されている場合、管理されている回線情報をリストアップしてください。
- 回線一覧管理台帳は、一般的に院内の総務担当や情報システム担当、その他部門システム担当等で管理されているので、ご担当者様への問合せをお願いします。

外部ネットワーク接続点の洗い出し方　<STEP3>

3　各部門への問合せによる独自契約回線のリストアップ

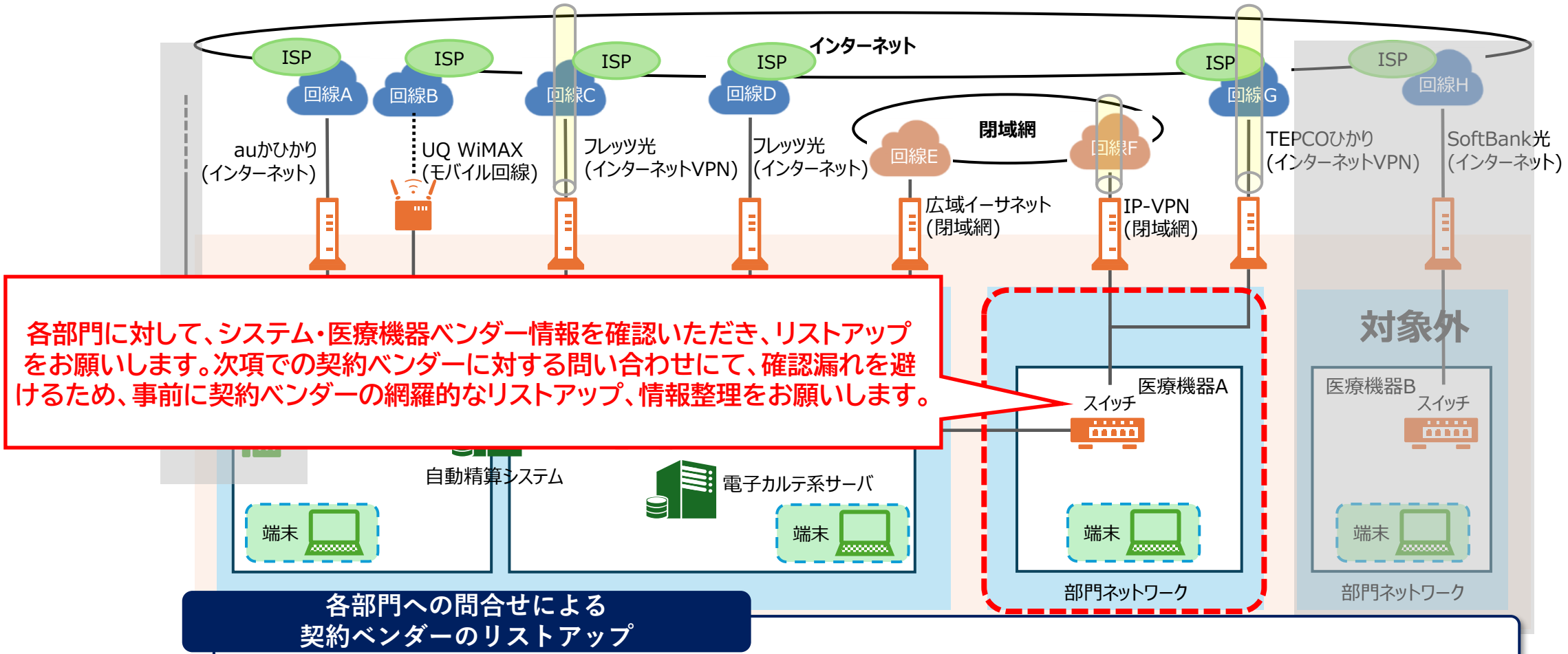


各部門への問合せによる独自契約回線のリストアップ

- 院内の総務部門や情報システム部門を介さずに、独自に契約した回線があるか、各部門への問合せ、リストアップをお願いします。
- 医療機器を導入した場合などに、医療機器ベンダーが保守回線を準備することが多くあります。

外部ネットワーク接続点の洗い出し方　<STEP4>

4　各部門への問合せによる契約ベンダーのリストアップ

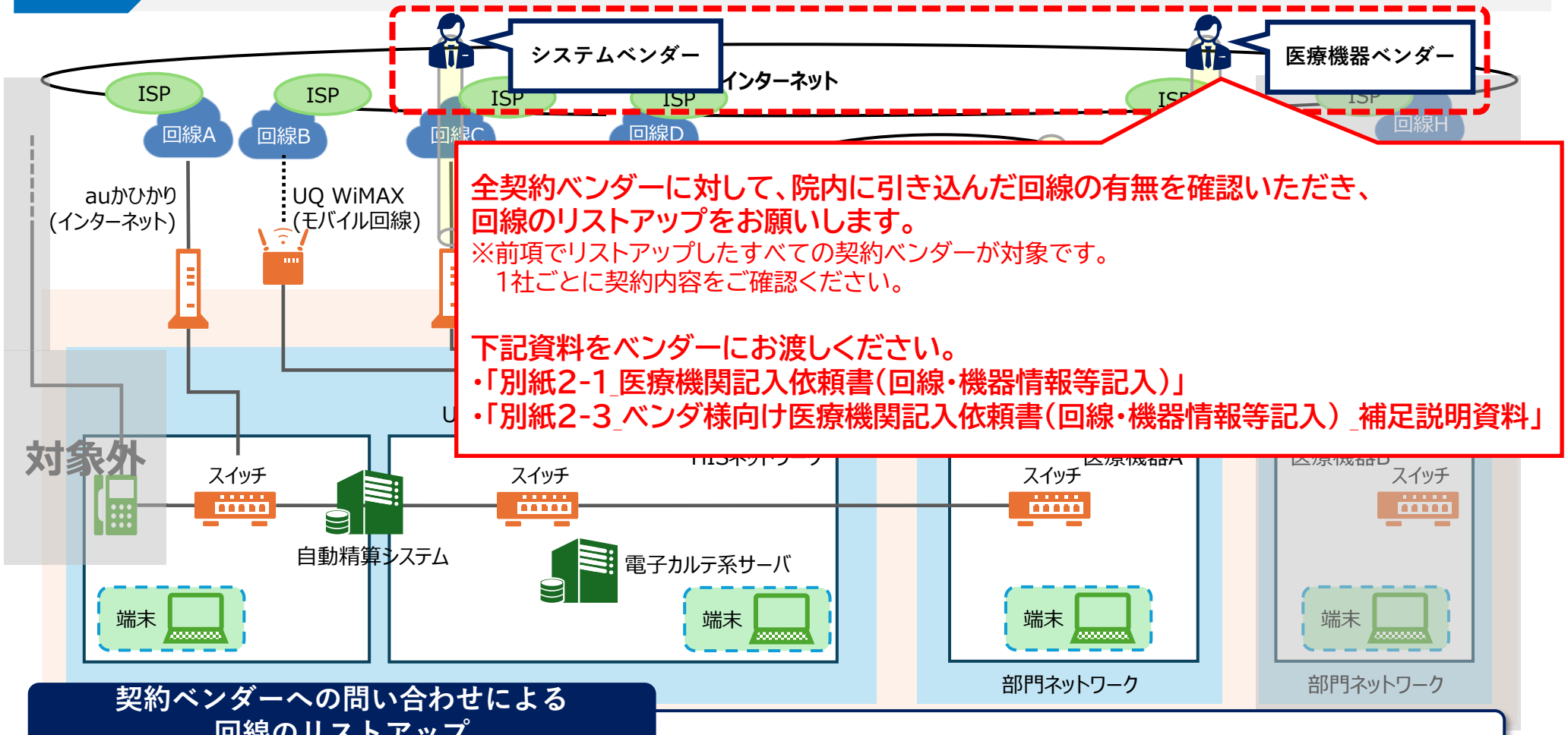


各部門への問合せによる契約ベンダーのリストアップ

- どのベンダーと契約をしているか各部門への問合せをし、システム・医療機器ベンダー情報のリストアップをお願いします。※契約しているベンダーすべてをリストアップしてください。
- 次項での問い合わせ漏れを避けるために、事前の情報整理をお願いします。

外部ネットワーク接続点の洗い出し方　<STEP5>

5　契約ベンダーへの問い合わせによる回線のリストアップ

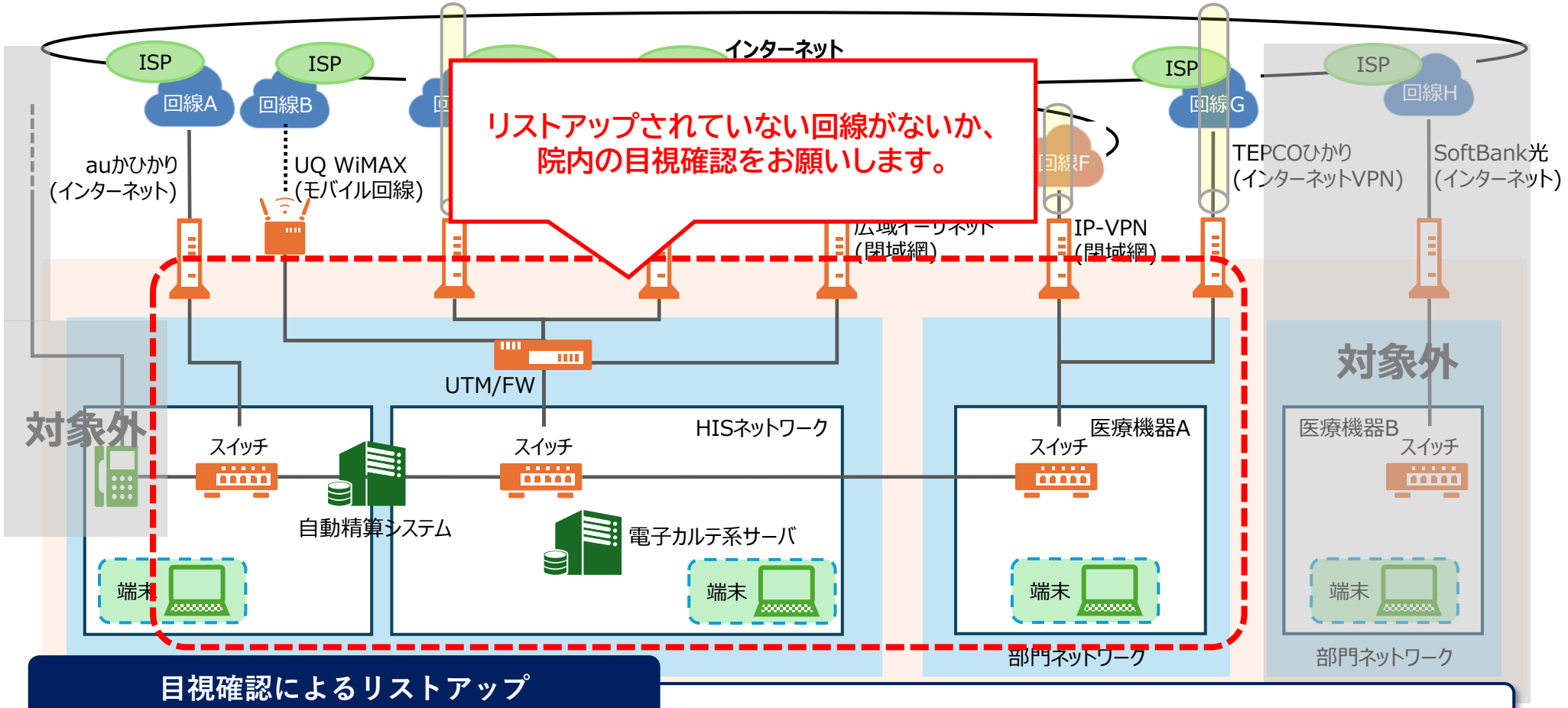


契約ベンダーへの問い合わせによる回線のリストアップ

- システム・医療機器ベンダーに確認し、院内に引き込んだ回線情報をリストアップしてください。
- 医療機関名義の回線だけではなく、ベンダー名義の回線も含め、電子カルテシステムに接続している回線すべてを対象とします。

外部ネットワーク接続点の洗い出し方　<STEP6>

6　目視確認によるリストアップ



目視確認によるリストアップ

- サーバ室をはじめ、各部門の居室を確認しただき、リストアップされていない回線（回線終端装置、モバイル回線接続機器）がないか、院内の目視確認をお願いします。

外部ネットワーク接続点の洗い出し方　<STEP6>

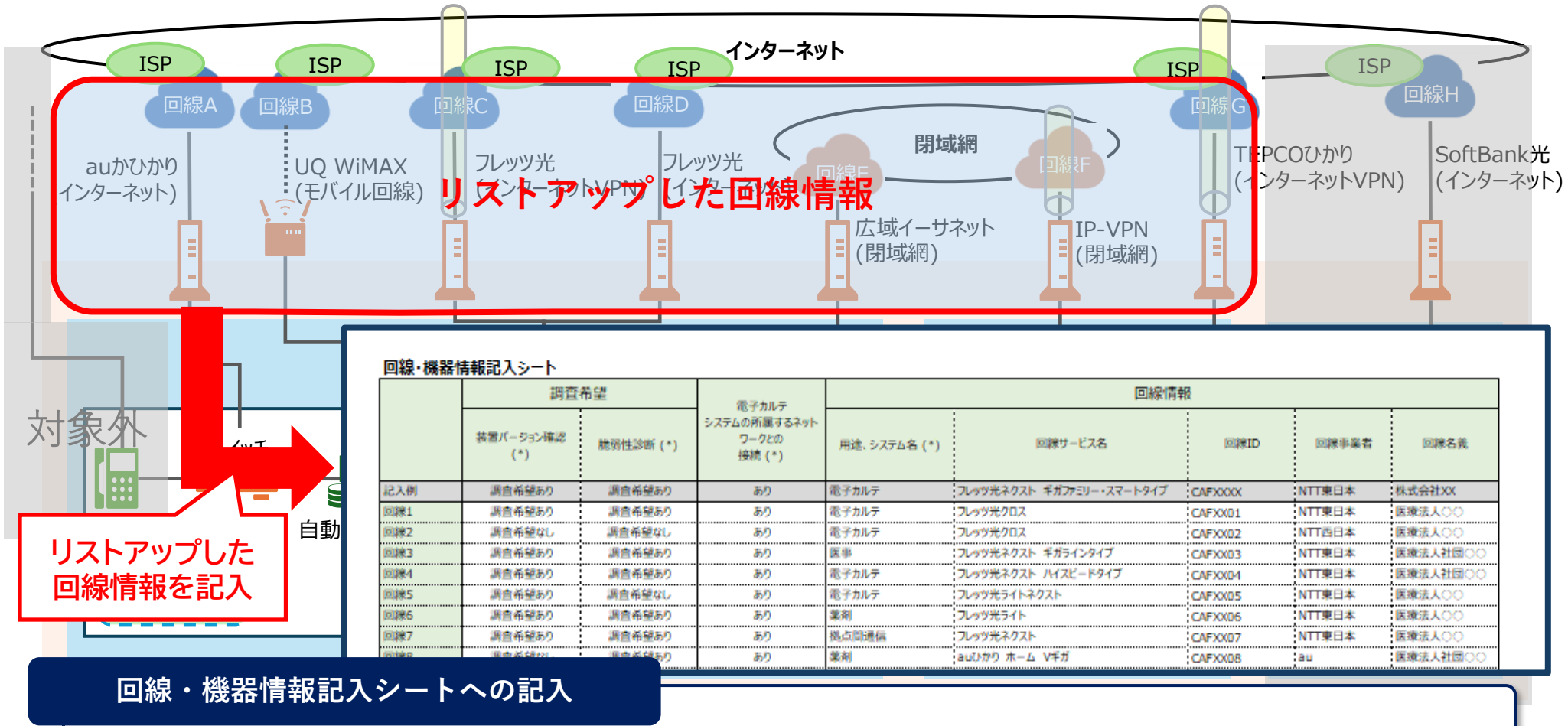
6　目視確認によるリストアップ

- 院内の目視確認をする際は、下記のような装置をあるか確認をお願いします。

	ONU (光回線終端装置)		CATVモデム
	HGW （ホームゲートウェイ）		ホームルーター ※モバイル回線
	CTU (加入者網終端装置)		モバイルルーター ※モバイル回線
	ADSLモデム		USBドングル ※モバイル回線

外部ネットワーク接続点の洗い出し方　<STEP7>

7　回線・機器情報記入シートへの記入



回線・機器情報記入シートへの記入

- リストアップした回線情報を、回線・機器情報記入シートへ記入をお願いします。
- 詳細は、「別紙2-2_医療機関情報記入依頼書（回線・機器情報等記入）補足説明資料」をご参照ください。

5. ご提出資料について

ご提出資料一覧

- **現地調査及びセキュリティ調査報告書を作成するために必要な情報となりますので、ご提出をお願いします。**

資料名	フォーマット	シート名	詳細説明	Check
①別紙2-1_医療機関記入依頼書（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。	□

基本情報記入シート

- **基本情報記入シートに記入していただきたい情報をご紹介いたします。**

1 本施策についての同意確認

「別紙7_医療機関におけるサイバーセキュリティ確保事業_規約」「別紙8_規約別紙_脆弱性診断における注意事項」をご確認いただき、“同意する”の選択をお願いします。

本事業の回答内容・調査結果が他の事業へ波及したり、医療機関様に不利益や不都合を与えるものではありません。

本施策の同意確認	(別紙)規約に記載の内容をご確認のうえ、本施策実施に同意いただける場合は「同意する」を選択してください	同意する

2 医療機関情報の記入

医療機関名、住所、病床数をご記入ください。

■お客様情報（医療機関情報）

医療機関名	(かな)					
住所	〒		住所	(かな)	ビル名	(かな)
病床数						

3 担当者情報の記入

担当者情報をご記入ください。担当者が複数名の場合を想定し、４名まで記入できる欄を設けています。

■医療機関 担当者情報（情報担当またはセキュリティ担当）※NTT東日本の事務局から連絡する際にご対応いただけるご担当者様

所属先		担当者名	(かな)	連絡先	
メールアドレス					

■医療機関 担当者情報（情報担当またはセキュリティ担当）※NTT東日本の事務局から連絡する際にご対応いただけるご担当者様

所属先		担当者名	(かな)	連絡先	
メールアドレス					

■医療機関 担当者情報（情報担当またはセキュリティ担当）※NTT東日本の事務局から連絡する際にご対応いただけるご担当者様

所属先		担当者名	(かな)	連絡先	
メールアドレス					

■医療機関 担当者情報（その他）

所属先		担当者名	(かな)	連絡先	
メールアドレス					

4 担当者の署名

最後に記入内容に不備がないかご確認いただき、担当者の署名をフルネームでご記入ください。

■申込内容の確認

確認者名(医療機関のご担当者名)	

✓ 現地調査に必要な住所や担当者などの基本情報の記入をお願いいたします。

✓ **別紙規約、計２部**
（「別紙7_医療機関におけるサイバーセキュリティ確保事業_規約」、「別紙8_規約別紙_脆弱性診断における注意事項」）を必ずご確認いただくようにお願いいたします。

回線・機器情報記入シート

- **回線・機器情報記入シートに記入していただきたい情報をご紹介いたします。**

1 調査希望・用途

現地で装置の調査、リモートで脆弱性診断を希望される場合は「調査希望あり」を選択してください。

回線・機器情報記入シート

	調査希望		電子カルテシステムの所属するネットワークとの接続 (*)	用途、システム名 (*)
	装置バージョン確認 (*)	脆弱性診断 (*)		
記入例	調査希望あり	調査希望あり	あり	電子カルテ
回線1	調査希望あり	調査希望あり	あり	電子カルテ
回線2	調査希望なし	調査希望あり	あり	電子カルテ
回線3	調査希望あり	調査希望あり	あり	医事

2 通信形態・アドレス

回線ごとに、グローバルIPに関する情報をご記入ください。

回線と紐付くグローバルIPアドレス						
通信形態 (*)	グローバルIP利用 (*)	固定IP/動的IP (*)	グローバルIPアドレス (*)	脆弱性診断当日記入欄		FQDN
				グローバルIP確認	グローバルIPアドレス	
インターネットVPN	あり	固定IP	121.119.249.222	入力不要	入力不要	example.xxx
インターネットVPN	あり	固定IP	0.0.0.0	入力不要	入力不要	○○.healthrecord
インターネットVPN	あり	固定IP	0.0.0.0	入力不要	入力不要	–
インターネット	あり	固定IP	0.0.0.0	入力不要	入力不要	–
インターネットVPN	あり	動的IP		確認済み	XXX.XXX.XXX.XXX	○○.eist

3 品目・設置場所

回線ごとに、品目名、回線終端装置の設置場所に関する情報をご記入ください。

プロバイダ情報		回線終端装置(ONU/モデム)情報
プロバイダ名	プロバイダ品目	回線終端装置設置場所 (*)
NTTぷらら	Bフレッツサービス	本部棟　3F　サーバー室　1番ラック　3U
AsahiNet	フレッツ光クロス	2F サーバー室A Bラック
		2F サーバー室A Bラック
		2F サーバー室A Bラック

4 機器情報

回線ごとに、関係する装置についての情報をご記入ください。

装置①※インターネット回線/ONUに紐づく装置(ルータ/UTM/FW)

装置の種類	メーカー (*)	機種名 (*)	レンタル装置 (*)	ファームウェアバージョン (*)	設置場所(*)	アカウント/パスワード (*)	パスワードポリシー確認					
							桁数 (*)	文字混在 (英数字、記号) (*)	推測困難な文字列 (*)	工場出荷時の設定から変更している (*)	他の機器と共通のパスワードを使用している (*)	定期的な変更 (*)
ルーター	Cisco	ISR 921	いいえ	15.1S	本部棟 3F サーバー室 1番ラック 7U	確認済み	13桁以上	混在あり	はい	はい	いいえ	なし
ルーター	不明	XG-100NE	はい	X.XX.XX	2F サーバー室A Aラック	確認済み	13桁以上	混在あり	はい	はい	いいえ	2ヶ月以内
ルーター	Cisco	ISR 921	いいえ	X.XX.XX	2F サーバー室A Bラック	確認済み	8-12桁	混在なし	いいえ	工場出荷時のパスワードを利用	いいえ	2ヶ月以内
ルーター	Cisco	ISR 1120	いいえ	X.XX.XX	2F サーバー室A Bラック	未確認						

装置②※「装置①」に紐づく装置(ルータ/UTM/FW)

装置の種類	メーカー (*)	機種名 (*)	レンタル装置 (*)	ファームウェアバージョン (*)	設置場所(*)	アカウント/パスワード (*)	パスワードポリシー確認					
							桁数 (*)	文字混在 (英数字、記号) (*)	推測困難な文字列 (*)	工場出荷時の設定から変更している (*)	他の機器と共通のパスワードを使用している (*)	定期的な変更 (*)
ファイアウォール/UTM	PaloAlto	PA-850	いいえ	11.1.1	本部棟 3F サーバー室 1番ラック 9U	確認済み	13桁以上	混在あり	はい	はい	いいえ	なし
ファイアウォール/UTM	PaloAlto	PA-3410	いいえ	XX.X.X	2F サーバー室A Aラック	確認済み	13桁以上	混在あり	はい	はい	はい	なし
ファイアウォール/UTM	Cisco	Firepower3110	いいえ	XX.X.X	2F サーバー室A Bラック	未確認						

- ✓ 回線情報と、回線に関わるネットワーク機器に関する情報の記入をお願いいたします。
- ✓ **回線を管理されている方、各部門システムの管理者、保守を依頼しているベンダーの方**などに情報の確認をお願いいたします。
- ✓ 詳細は「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認ください。

調査端末情報記入シート

- **調査端末情報記入シートに記入していただきたい情報をご紹介いたします。**

1 機器情報

端末ごとに、ホスト名やIPアドレスなどの詳細情報をご記入ください。

調査端末情報

	システム種別 (*)	シンクラ利用 (*)	シンクラ端末/FAT端末			仮想デスクトップ	
			端末ホスト名 (*)	IPアドレス(*)	設置場所 (*)	端末ホスト名	IPアドレス
記入例	電子カルテ	はい	PCXXXX	192.168.1.25/24	2F ○○室	PCXXXX	192.168.1.25/24
No.1	電子カルテ	はい	PCXXXX01	192.168.1.131/24	西棟 2F 診察室A-1	VDI-XXXX01	172.16.1.131/24

2 セキュリティ対策製品名

端末ごとに、ウイルス対策ソフト、EDRなどのセキュリティ対策製品名をご記入ください。

セキュリティ対策製品	
Microsoft Defender	
Trend Micro Apex One	

3 留意事項

端末操作可能時間などの留意事項がある場合は、備考に記入をお願いします。

備考
端末操作可能時間：12:00-13:00
端末操作時常時立ち合い必須

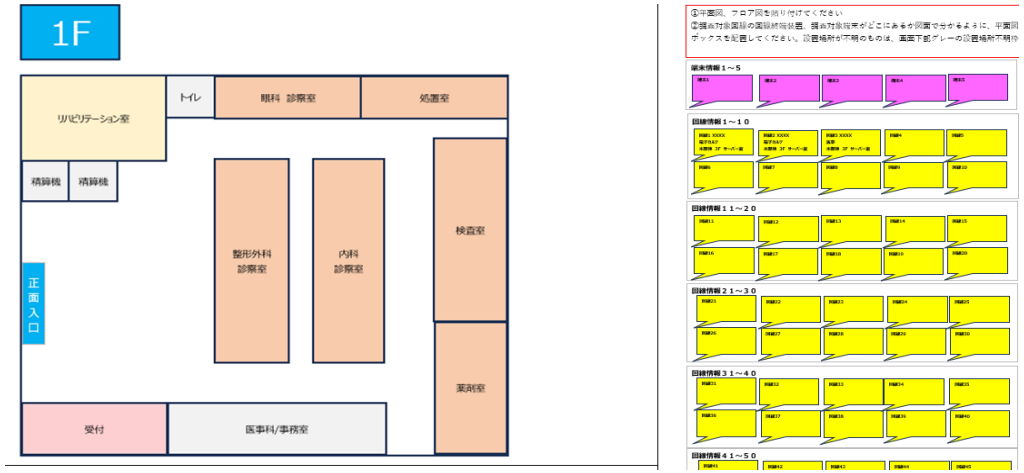
- ✓ 調査対象の端末(PC)に関する情報の記入をお願いいたします。
- ✓ **端末を管理されている方、各部門システムの管理者**などに情報の確認をお願いいたします。
- ✓ 詳細は「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認ください。

設置場所記入シート

- **設置場所記入シートに記入していただきたい情報をご紹介いたします。**

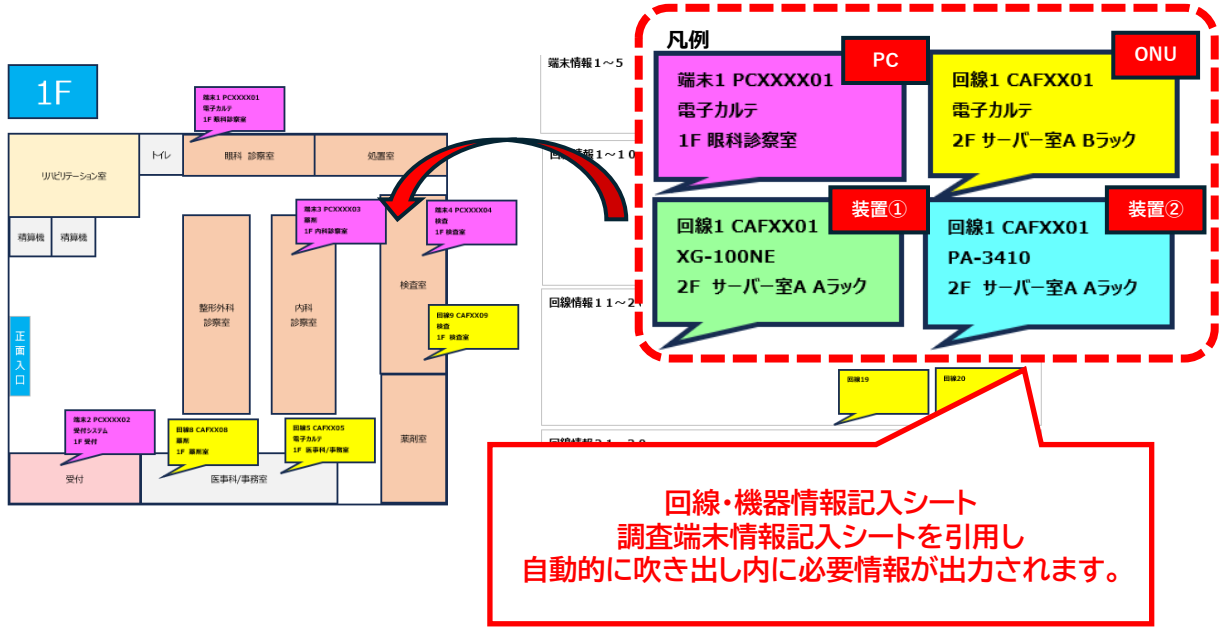
1 平面図画像の貼り付け

平面図の画像の貼り付けをお願いします。



2 平面図上に調査対象機器情報をプロットする

調査対象回線の回線終端装置、調査対象端末の情報が入った吹き出しを平面図上に配置し、それらがどこに設置されているか、現地調査員が分かるようにしてください。



- ✓ 調査対象の回線終端装置、調査対象端末の設置位置が、平面図を見て分かるように、吹き出しの配置をお願いいたします。
- ✓ 回線・機器情報記入シート、調査端末情報記入シートを記入いただくことで、自動的に吹き出し内に情報が出力されます。
- ✓ 詳細は「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認ください。

アカウント(ログインID)・パスワードリスト

・アカウント(ログインID)・パスワードリストに記入していただきたい情報をご紹介いたします。

1 調査対象装置・端末のログイン情報の整理

調査対象装置・端末のアカウント/ログインID、パスワードの整理をお願いします。

■ **装置①** ※インターネット回線/ONUに紐づく装置(ルータ/UTM/FW)

	メーカー	機種名	アカウント/ログインID	パスワード	特権(enable)モード パスワード
回線1	不明	XG-100NE			
回線2	Cisco	ISR 921			
回線3	Cisco	ISR 1120			
回線4	Fujitsu	Si-R570B			
回線5	Paloalto	PA-410			

■ **調査端末 (シンクラ端末/FAT端末)**

	端末ホスト名	IPアドレス	アカウント	パスワード
端末1	PCXXXX01	192.168.1.131/24		
端末2	PCXXXX02	172.16.10.151/28		
端末3	PCXXXX03	10.0.10.101/24		
端末4	PCXXXX04	172.16.20.172/24		
端末5	PCXXXX05	192.168.50.201/24		

2 注意事項、補足事項の記入

接続先情報や、留意事項などがあれば備考欄にご記入ください。

備考 (接続先情報など)

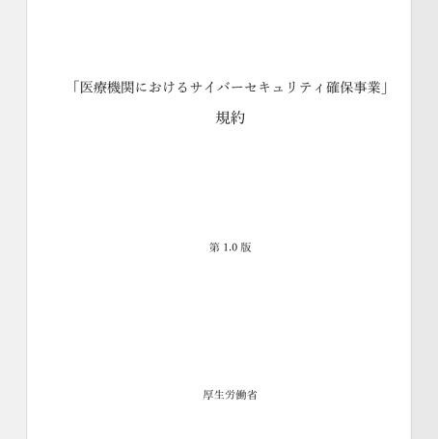
提出不要

- ✓ 調査対象の回線終端装置、調査対象端末へのログイン情報の整理をお願いします。
- ✓ **アカウント(ログインID)・パスワードリストは、弊社への提出は不要です。**作業当日までに情報整理していただくことを目的としています。**アカウント・パスワードが不明の場合、調査は不可能となり、現地調査の精度も低下します。**現地調査当日までに忘れずに情報を準備していただくよう、ご協力をお願いします。
- ✓ 詳細は「別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料」をご確認ください。

本事業における規約

- **本事業を実施するにあたっての、役務内容、免責事項、情報取り扱い等をとりまとめた規約を準備しています。**
- **本規約をご一読いただき、「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の同意欄で「同意する」を選択の上で提出をお願いします。**

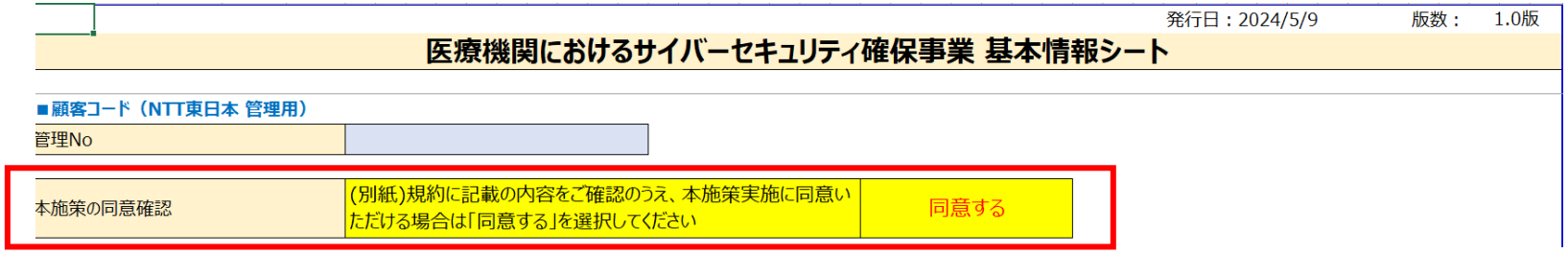
規約の確認


「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

- **配布している、「別紙7_医療機関におけるサイバーセキュリティ確保事業_規約」をご確認ください。**
- **この規約には、本事業で提供される役務内容、免責事項、前提条件等が記載されています。**

同意確認欄へ記入

配布しているExcel「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の基本情報記入欄において、“同意する“を選択の上、ご提出ください。


発行日：2024/5/9　　版数：　1.0版

医療機関におけるサイバーセキュリティ確保事業 基本情報シート

■顧客コード（NTT東日本 管理用）

管理No	

本施策の同意確認	(別紙)規約に記載の内容をご確認のうえ、本施策実施に同意いただける場合は「同意する」を選択してください	同意する

6. 事務局連絡先

事務局連絡先

２０２４年７月４日から受付開始しております。

本事業の事務局連絡先

本説明会内容に関する問合せ、その他ご不明な点がありましたらお問い合わせください

pj-mhlw-gm@east.ntt.co.jp

03-6915-4268　平日（月～金）　９時３０分～１７時００分

お電話がつながりにくい場合がありますので、可能な限りメールにてご連絡をお願いします。
問合せ内容によって、ご回答にお時間をいただく場合がございます。

参考. Q&A

Q&A

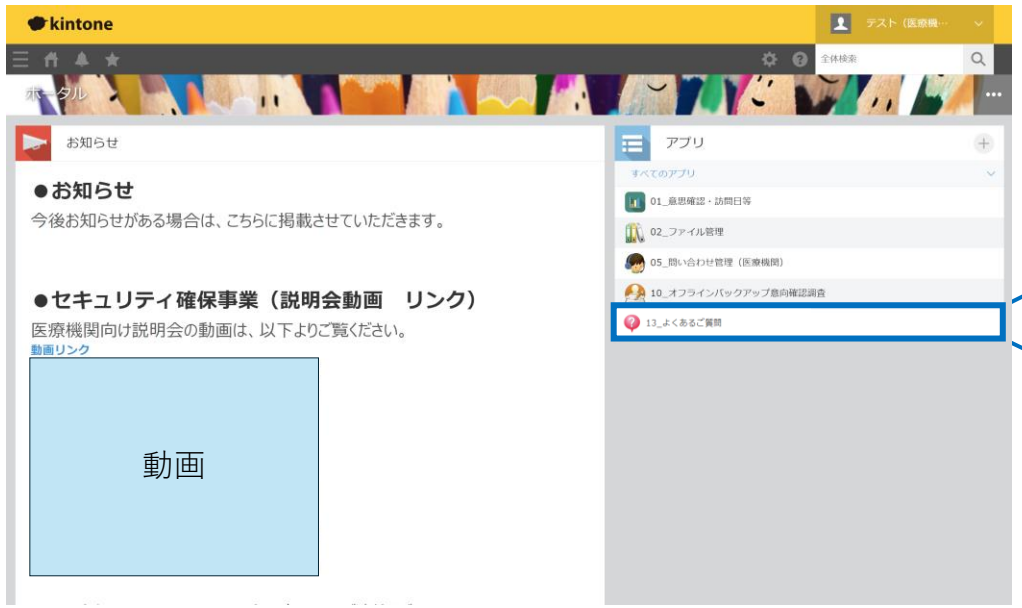
No	質問	回答
1	本事業で病院から提供する情報は機密情報にあたるが、情報の取り扱いについて教えてほしい。	厚生労働省「別紙7_医療機関におけるサイバーセキュリティ確保事業_規約」に情報の取り扱い含め、以下の内容を規定しております。 本規約は事務局より各医療機関様へ送付しますので、本事業に参画にあたって予めご確認いただき、「別紙2-1_医療機関記入依頼書（回線・機器情報等記入）」の同意確認欄へのチェックをお願いします。（P47参照） ＊規約の目次（抜粋） 1. 本規約の目的 2. 定義 3. 役務内容 4. 免責事項等 5. 禁止事項 6. 本役務の変更、中止等 7. 秘密保持 8. 知的財産 9. 損害賠償 10. 規約改定 11. 本規約上の地位の譲渡等 12. 紛争解決 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
2	外部ネットワーク接続の俯瞰的把握、安全性の検証・調査の対象はどの範囲か。	リモート保守用の回線や、閉域網、無線等、基幹（電子カルテ）系につながるすべての出入り口が調査対象です。（電子カルテシステムから独立しているネットワークは調査対象外です）（P6参照）
3	本事業での回答内容や調査結果が他の事業へ影響を与えるものか。	本事業は、外部接続を中心としたセキュリティの現状把握と今後の課題を各医療機関様に認識いただくことを目的としています。本事業の回答内容・調査結果が他の事業へ波及したり、医療機関様に不利益や不都合を与えるものではありません。

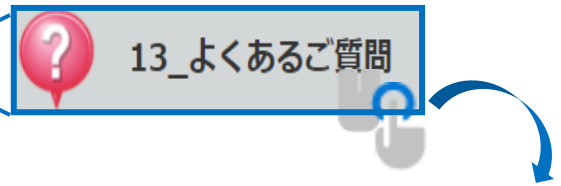
Q&A

No	質問	回答
4	本事業の支援A（※1）、支援B（※2）及び支援C（※3）には、診療録管理体制加算1の要件とされている、バックアップの「複数方式」での確保及び「オフライン」での保管に関する内容が含まれていると考えてよいか。 ※1 既存バックアップの状況確認、オフラインバックアップ計画・運用手順の策定支援、ゲートウェイサーバ、バックアップ媒体のセットアップ、設置 ※2 既存バックアップの状況確認、オフラインバックアップ計画・運用手順の策定支援、ゲートウェイサーバ、バックアップ媒体のセットアップ手順、設置手順の提供 ※3 既存バックアップの状況確認、オフラインバックアップ計画・運用手順の策定支援	よい。ただし、支援B、Cについては、あくまで計画・手順を示すものであって、具体的な体制構築及び運用に対する直接的な支援は含まれないことに留意されたい。

その他のQ＆A

- **その他のQ＆Aは、「セキュリティ確保事業ポータル」内の以下のアクセス先よりご確認ください。順次、追加予定です。**
- **ポータルトップ画面の右下「13_よくあるご質問」をクリックしてご確認いただけます。是非ご活用ください。**





参考. 資料の構成

資料の構成

6/25修正

本日7/3時点での医療機関様へのご提供資料一式は以下のとおりです。
今後追加の資料が発生する場合には、ポータルシステムへの掲載、事務局からメールにてご連絡します。

資料名	概要
本編_医療機関向け説明資料	本資料。本事業の概要、実施フローなどの詳細説明資料。
別紙1-1_外部接続点の洗い出し方	外部接続点の洗い出し方の解説書。本資料の「４．外部接続点の洗い出し」と同様の内容を記載しています。
別紙2-1_医療機関記入依頼書（回線・機器情報等記入）	「外部ネットワーク接続の俯瞰的把握、安全性の検証・調査」の実施にあたって、医療機関の皆様に必要な情報を記入いただくフォーマット。
別紙2-2_医療機関記入依頼書（回線・機器情報等記入）補足説明資料	医療機関の担当者様向け別紙2-1の記入にあたっての解説書。
別紙2-3_ベンダ様向け医療機関記入依頼書（回線・機器情報等記入）補足説明資料	医療機関ベンダー様向け別紙2-1の記入にあたっての解説書。
別紙3_ベンダ様向けNW機器調査説明資料	「外部ネットワーク接続の俯瞰的把握、安全性の検証・調査」のNW機器調査にあたって、医療機関ベンダーにご確認いただく資料。
別紙4_ベンダ様向け脆弱性診断説明資料	「外部ネットワーク接続の俯瞰的把握、安全性の検証・調査」の脆弱性診断の実施にあたって、医療機関ベンダーにご確認いただく資料。
別紙5_各媒体におけるオフライン状態の定義	本事業でのオフラインバックアップの定義についての解説書。
別紙6_オフラインバックアップ支援可能物品一覧	本事業でのオフラインバックアップの構築支援物品一覧。
別紙7_医療機関におけるサイバーセキュリティ確保事業_規約	本事業における規約。ご参画にあたって必ずご一読ください。
別紙8_規約別紙_脆弱性診断における注意事項	別紙７の規約の別紙。ご参画にあたって必ずご一読ください。