

2025年5月9日(金)
厚生労働省 医政局 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

ヒアリングシート補足資料

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. ヒアリングシートについて P 3 ~
2. ヒアリングシート作成方法 P 5 ~
3. 基本情報シートの作成 P 11 ~
4. 回線情報シートの作成 P 14 ~
5. 端末情報シートの作成 P 30 ~
6. 設置場所情報シートの作成 P 42 ~
7. 追加説明資料 P 47 ~



1. ヒアリングシートについて



ヒアリングシートとは・目的

1. ヒアリングシートについて

- 厚生労働省委託事業である「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)」では、以下に示す2つの調査を実施いたします。
 - 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
 - ②オンラインバックアップ体制の整備支援

※「②オンラインバックアップ体制の整備支援」につきましては、別途アンケート等でヒアリングさせていただきます。
- 「ヒアリングシート」は、上記2つの調査のうち、
「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」を実施するためにご提出いただくExcelファイルのことを指します。
- ヒアリングシートの目的は以下となります。
 - ・外部接続を中心としたセキュリティの現状を把握していただくこと
- 提出いただいた情報をもとに、現地調査、脆弱性診断を実施し、調査報告書を作成いたします。
- **本事業における回答内容・調査結果について、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たりするものではありません。**



2. ヒアリングシート作成方法



ヒアリングシートにおける注意事項

2. ヒアリングシート 作成方法

- ・ ヒアリングシートを作成いただくにあたり注意していただきたい4点について、以下に記載しております。ご一読のうえ、ヒアリングシートの作成をよろしくお願ひいたします。

① 電子カルテシステムとの接続がある回線のみ記入する。

- ・ 回線情報シートには、電子カルテシステムへの接続がある回線をご記入いただくことを前提としております。

② ヒアリングシートのファイル名を変更してから対応する。

- ・ ヒアリングシートのファイル名を変更したのち、ヒアリングシートの記入を開始してください。

③ ヒアリングシートのファイル名における命名規則に注意する。

- ・ ヒアリングシートのファイル名については、以下のようにご変更ください。

通番_医療機関名_ヒアリングシート_日付.xlsx

- ・ 通番： 本事業で貴院に割り当てられた通番を4桁でご記入ください。

例) 321⇒「0321」

※メール件名に管理番号【通番:●●●●】を付与しております。こちらの通番をご記入ください。

- ・ 医療機関名： 貴院の医療機関名を正式名称で、空欄を入れずにご記入ください。

- ・ 日付： 本資料を提出いただく日付を「YYYYMMDD」の形式でご記入ください。

例) 通番:2000、医療機関名:NTTテスト病院、提出日付:2025年5月22日 の医療機関の場合

2000_NTTテスト病院_20250522.xlsx

※ファイル名について、0000 NTTサンプル病院 ヒアリングシート 20250522.xlsx の形としていただきますようお願ひいたします。

④ ヒアリングシート内における行・列・セルの取り扱いに注意する。

- ・ ヒアリングシート内の各シートについて、行/列の追加/削除はお控えください。

- ・ ヒアリングシート内の各セルについて、追加/削除/結合はお控えください。

ヒアリングシートにおけるシート

2. ヒアリングシート 作成方法

- ・ ヒアリングシートには、「0.留意事項」「1.基本情報」「2.回線情報」「3.端末情報」「4.設置場所情報」の5つのシートがあります。
- ・ 「0.留意事項」を除く4シートにおける必要箇所すべてに情報をご記入ください。

■ ヒアリングシートでは、以下4つのシートに情報をご記入ください。

– 1. 基本情報

医療機関情報を記入いただくシート

– 2. 回線情報

電子カルテに接続されている回線と、その回線に紐づく機器をご記入いただくシート

– 3. 端末情報

電子カルテシステムの端末、その他医療情報システムの端末の情報を記入いただくシート

– 4. 設置場所情報

「2.回線情報」「3.端末情報」で記載いただいた機器/端末の設置場所を、平面図上に示していただくシート

これらのシートにおける必要箇所すべてに情報をご記入ください。
※原則、全箇所への記入が必要です。

ヒアリングシート作成の流れ

2. ヒアリングシート 作成方法

- ヒアリングシートは4つのシートから構成されています。それぞれのシートに対して、必要情報の入力をお願いいたします。

基本情報シート

回線情報シート

端末情報シート

設置場所情報シート

基本情報の記入

医療機関名、メイン担当者・立会者情報などを記入する。

回線についての基本情報の記入

洗い出した回線情報を記入する。

脆弱性診断関連の情報の記入

脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。

回線に紐づく機器情報の記入

記入した回線に紐づくネットワーク機器の情報を記入する。

各機器における パスワードポリシーの記入

記入した機器におけるパスワードポリシーを記入する。

端末についての基本情報の記入

電子カルテ・医療情報システムで使用している端末情報を記入する。

セキュリティ対策状況・ パスワードポリシーの記入

記入した端末におけるセキュリティ対策状況、パスワードポリシーを記入する。

機器の設置場所を示す 平面図の作成

回線情報シート、端末情報シートにて記入した機器の設置場所を平面図上にあらわす。

ヒアリングシート内のルール

2. ヒアリングシート 作成方法

- ・ヒアリングシートの記入欄は、記入箇所を明示するために色分けを行っております。ヒアリングシートご記入の際には、ご一読ください。
- ・グレーアウトされている記入欄については、入力していただく必要はございません。

ヒアリングシート内の表記		表記の意味
項目欄		項目欄が 緑 ⇒記入いただいた情報をもとに、現地調査を実施いたします。
記入欄		項目欄が オレンジ ⇒記入いただいた情報をもとに、脆弱性診断を実施いたします。
項目欄		項目欄が 青 ⇒記入いただいた情報をもとに、調査報告書を作成いたします。
記入欄		記入欄が 白 ⇒確認した情報の記入をお願いいたします。
記入欄		記入欄が オレンジ ⇒分岐があった際に着色されます。記入をお願いいたします。

本資料における凡例

2. ヒアリングシート 作成方法

- 以下に、本資料(ヒアリングシート補足資料_YYYYMMDD.pptx)にて使用している表記の説明を記載しております。

凡例	表記の意味
○○調査 △△を選択した場合	前の回答項目により発生した分岐先を示しています。 ※分岐が重なる際は、枠線の色を異なるものにしています。
□□にて 「～～～」を選んだ場合	該当スライドにて注意事項があることを示しています。
○○の場合でも ご回答ください	該当スライドと関連するスライドのタイトルを、「:」以降に 記載しています。
関連スライド :○○の情報の記入③,④	



3. 基本情報シートの作成



基本情報記入シートのヒアリング内容

3. 基本情報シートの作成

- 基本情報シートでは、以下の内容をヒアリングさせていただきます。

- 医療機関の情報
- 本事業のメインのご担当者様の連絡先
- 現地調査時の立会者様の連絡先
- 現地調査時に必要な情報

基本情報シート	回線情報シート	端末情報シート	設置場所情報シート
基本情報の記入 医療機関名、メイン担当者・立会者情報などを記入する。	回線についての基本情報の記入 洗い出した回線情報を記入する。	端末についての基本情報の記入 電子カルテ・医療情報システムで使用している端末情報を記入する。	機器の設置場所を示す平面図の作成 回線情報シート、端末情報シートにて記入した機器の設置場所を平面図上にあらわす。
脆弱性診断関連の情報の記入 脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。	回線に紐づく機器情報の記入 記入した回線に紐づくネットワーク機器の情報を記入する。 各機器におけるパスワードポリシーの記入 記入した機器におけるパスワードポリシーを記入する。	セキュリティ対策状況・パスワードポリシーの記入 記入した端末におけるセキュリティ対策状況、パスワードポリシーを記入する。	

基本情報の記入①

3. 基本情報シートの作成

医療機関名等の基本情報と、現地調査を行うにあたって必要な情報をご記入いただきます。

■ 通番(記載不要)

貴院の通番が記入される欄です。ヒアリングシートのファイル名を変更すると自動的に記入されるため、新たにご記入いただく必要はございません。

■ 医療機関名・住所

医療機関名と住所をご記入ください。

※あわせて”かな”の記入もお願いいたします。

■ 連絡先情報(本事業におけるメイン担当者様)

本事業におけるメインのご担当者様の連絡先をご記入ください。

■ 連絡先情報(現地調査時の立合者様)

現地調査時に立ち合いただける方の連絡先をご記入ください。

※メイン担当者様が立会者様となる場合、ご記入いただく必要はございません。

■ 駐車場の有無

駐車場の有無についてプルダウンメニューよりお選びください。

■ 当日の連絡手段の貸し出し(PHS等)

貸出可否が確定している場合、「はい」または「いいえ」をお選びください。

確定していない場合、「現地にて確認」をお選びください。

■ 備考

その他、現地調査を実施する際の留意事項があれば、その内容をご記入ください。

1. 基本情報			
医療機関情報			
通番 (記載不要)			
医療機関名	(かな) 様		
住所	〒 (かな)		
連絡先情報 (本事業におけるメイン担当者様)			
担当者氏名 (フルネーム)	(かな) 様		
部署名			
電話番号			
メールアドレス			
連絡先情報 (現地調査時の立合者様) ※メイン担当者様が立会者様となる場合は記載不要			
担当者氏名 (フルネーム)	(かな) 様		
部署名			
電話番号			
メールアドレス			
現地調査における確認事項			
入館に関する確認事項			
駐車場の有無		利用時の注意点	
当日の連絡手段の貸し出し(PHS等)	現地にて確認	特記事項	
その他			
備考			



4. 回線情報シートの作成



回線情報記入シートのヒアリング内容

4. 回線情報シートの作成

- 回線情報シートでは、以下の内容をヒアリングさせていただきます。

- 回線に関する基本情報
- 脆弱性診断希望有無、通信形態（希望ありの場合：グローバルIPアドレスの情報）
- 回線に紐づく機器（最大2台）のメーカー名、型番、シリアルナンバーの情報
- 回線に紐づく機器のパスワードポリシー

基本情報シート	回線情報シート	端末情報シート	設置場所情報シート
<p>基本情報の記入 医療機関名、メイン担当者・立会者情報などを記入する。</p> <p>回線についての基本情報の記入 洗い出した回線情報を記入する。</p> <p>脆弱性診断関連の情報の記入 脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。</p> <p>回線に紐づく機器情報の記入 記入した回線に紐づくネットワーク機器の情報を記入する。</p> <p>各機器におけるパスワードポリシーの記入 記入した機器におけるパスワードポリシーを記入する。</p>	<p>回線についての基本情報の記入 洗い出した回線情報を記入する。</p> <p>脆弱性診断関連の情報の記入 脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。</p> <p>回線に紐づく機器情報の記入 記入した回線に紐づくネットワーク機器の情報を記入する。</p> <p>各機器におけるパスワードポリシーの記入 記入した機器におけるパスワードポリシーを記入する。</p>	<p>端末についての基本情報の記入 電子カルテ・医療情報システムで使用している端末情報を記入する。</p>	<p>機器の設置場所を示す平面図の作成 回線情報シート、端末情報シートにて記入した機器の設置場所を平面図上にあらわす。</p>

回線基本情報の記入①

4. 回線情報シートの作成

回線についての基本情報をご記入いただきます。「2.回線情報」シートの【回線情報】に該当します。

■ 申告回線No.

ご申告いただく回線について、番号を付与する欄です。
新たに何かをご記入いただく必要はございません。
※現地調査時や、調査報告書等で使用いたしますため、
医療機関様にて変更いただかないようお願いいたします。

■ 回線サービス名

回線サービス名をご記入ください。
回線契約時の契約書や請求書等で確認することができます。
院内における回線の管理ご担当者様や、ベンダ様にご確認
いただくことも有効です。

■ 回線サービスのID(CAF番号等)

該当する回線サービスについて、回線IDや回線契約番号を
ご記入ください。

回線サービスのIDについて、以下のようなものが該当します。

例1)CAF番号:CAFから始まる、全13桁の番号
⇒(CAF+数字10桁)

例2)COP番号:COPから始まる、全11桁の番号
⇒(COP+数字8桁)

※例1,2に該当する番号が存在しない場合、
回線を識別できる番号をご記入ください。

※回線情報を記入する際は、同じ回線サービスIDを並べて、
順番に記入するようお願いいたします。

例)CAF番号、COP番号から先に記載

※現地調査時に回線の並び順を変更させていただく場合がございます。

申告回線 No.	回線情報			
	回線サービス名	回線サービスのID (CAF番号等)	回線終端装置設置場所	用途、システム名
例	フレッツ光ネクスト ギガファミリー・スマートタイプ	CAF1111111111	本部棟 3F サーバー室 1番ラック 3U	電子カルテシステム
01	VPN接続サービス	CAF1111111111	1F サーバ室	電子カルテシステム
02	VPN接続サービス	CAF1111111111	1F サーバ室	地域医療連携システム
03	VPN接続サービス	CAF1111111111	1F サーバ室	部門システム
04	フレッツ光ネクスト ギガファミリー・スマートタイプ	CAF2525252525	本部棟 3F サーバー室 1番ラック 3U	医療機器
05	○○ △△タイプ	COP88888888	2F 医事課	医療事務・会計システム

回線基本情報の記入②

4. 回線情報シートの作成

回線についての基本情報をご記入いただきます。「2.回線情報」シートの【回線情報】に該当します。

■ 回線終端装置設置場所

各回線を引き込むための機器であるONUやモ뎀などの設置場所や設置位置をご記入ください。

ラックに設置されている場合は、ラック番号、ユニット番号など、できるだけ詳しい設置場所をご記入ください。
詳細な設置場所をご記入いただくことで、当日の作業がスムーズになります。ご協力をお願いいたします。

■ 用途・システム名

該当する回線に紐づく医療情報システムについて、プルダウンメニューよりお選びください。

※プルダウンメニューにある内容について、どの用途、システム名が当てはまるかについては、7. 追加説明資料【補足①:用途、システム名】をご参照ください。

申告回線 No.	回線情報			
	回線サービス名	回線サービスのID (CAF番号等)	回線終端装置設置場所	用途、システム名
例	フレッツ光ネクスト ギガファミリー・スマートタイプ	CAF1111111111	本部棟 3F サーバー室 1番ラック 3U	電子カルテシステム
01	VPN接続サービス	CAF1111111111	1F サーバ室	電子カルテシステム
02	VPN接続サービス	CAF1111111111	1F サーバ室	地域医療連携システム
03	VPN接続サービス	CAF1111111111	1F サーバ室	部門システム
04	フレッツ光ネクスト ギガファミリー・スマートタイプ	CAF2525252525	本部棟 3F サーバー室 1番ラック 3U	医療機器
05	○○ △△タイプ	COP88888888	2F 医事課	医療事務・会計システム

脆弱性診断関連の情報の記入①

4. 回線情報シートの作成

脆弱性診断関連の情報を記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

■ 脆弱性診断希望

グローバルIPアドレスを持つ機器に対して、遠隔地からリモート接続により脆弱性調査を実施いたします。

脆弱性診断を希望される場合は「調査希望あり」をお選びください。
※各ベンダ様と医療機関様でご相談のうえ、脆弱性診断希望有無を選択いただきますようお願いいたします。

脆弱性診断						
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック (記入不要)	グローバルIPアドレス 設定機器
診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に問題ございません。	機器A
診断希望あり	インターネット	固定IP	111.111.111.111	/32	記載に問題ございません。	機器A
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。			機器B
	閉域網					

脆弱性診断関連の情報の記入②

4. 回線情報シートの作成

脆弱性診断関連の情報を記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

■ 通信形態

通信形態について、「インターネット」、「インターネットVPN」、「閉域網」のいずれかをプルダウンメニューよりお選びください。

1回線で複数の通信形態がある場合、

各通信形態ごとに行を分けてご記入ください。

「閉域網」を選択した際にグレーアウトされる記入欄について、ご記入いただく必要はございません。

※通信形態の詳細については、

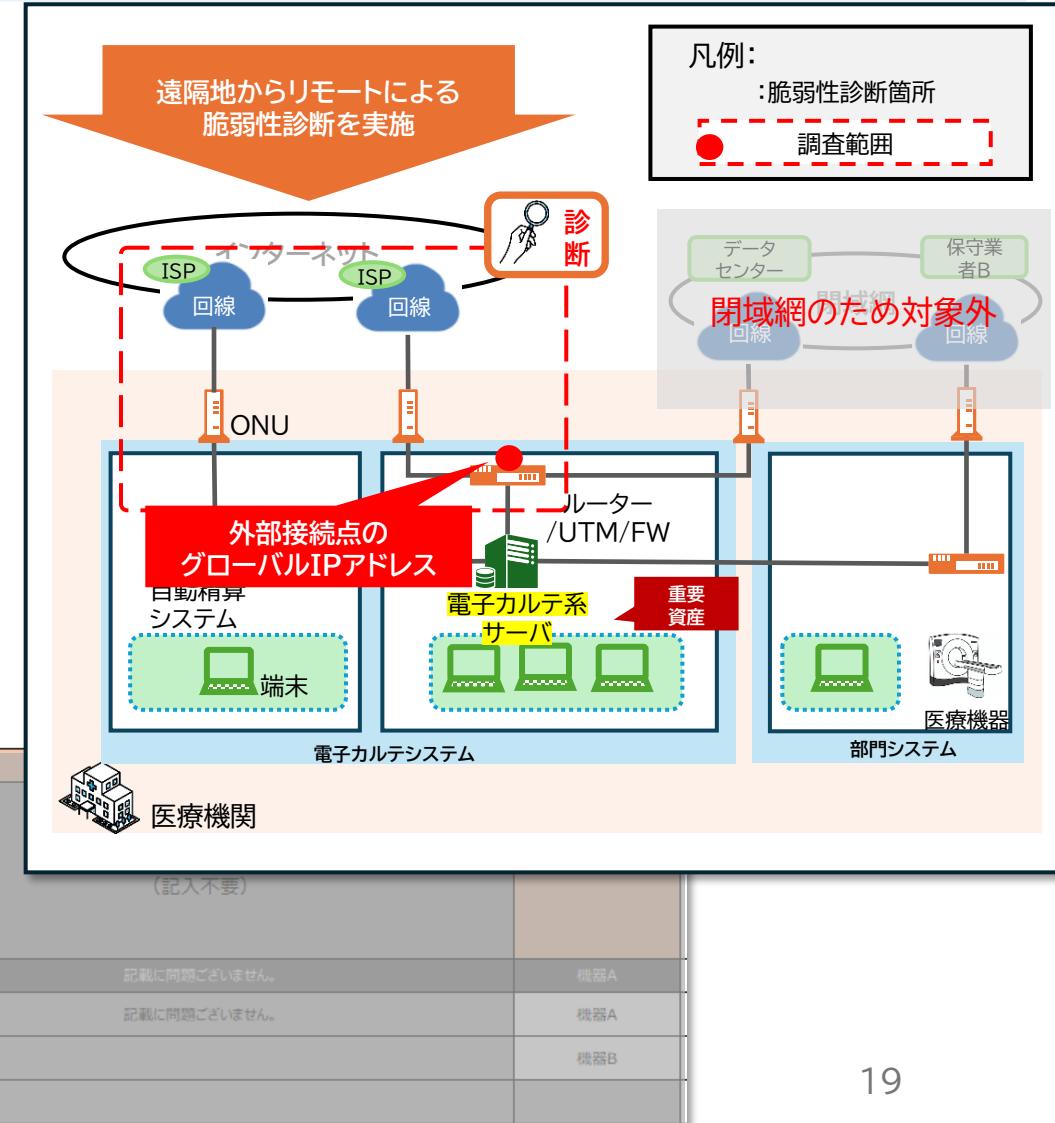
7. 追加説明資料【補足③:通信形態】をご参照ください。

※以下のバージョンのヒアリングシートでは、「通信形態」がグレーアウトされている場合がございます。

その場合でも、プルダウンメニューより通信形態をお選びください。

- ・「[通番]_[医療機関名]_ヒアリングシート_20250509.xlsx」
- ・「別紙1_[通番]_[医療機関名]_ヒアリングシート_20250509.xlsx」

脆弱性診断				
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長
診断希望あり	インターネット	固定IP	121.119.249.222	/32
診断希望あり	インターネット	固定IP	111.111.111.111	/32
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。	
	閉域網			



脆弱性診断関連の情報の記入③

4. 回線情報シートの作成

脆弱性診断関連の情報をご記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

- 「脆弱性診断」欄における以下の項目は、「脆弱性診断希望」欄にて「診断希望あり」を選択された場合に記載・確認いただく項目となります。

「固定IP/動的IP」
「グローバルIPアドレス」
「プレフィックス長」
「入力チェック(記入不要)」
「グローバルIPアドレス設定機器」

■ 脆弱性診断: 実施希望ありの場合

⇒「脆弱性診断希望」欄にて、「診断希望あり」をプルダウンメニューから選択
⇒[【脆弱性診断関連の情報の記入④】](#)へ

■ 脆弱性診断: 実施希望なしの場合

⇒「脆弱性診断希望」欄を空欄のままする
⇒[【回線に紐づく機器情報の記入①】](#)へ

※脆弱性診断の補足説明

⇒[7. 追加説明資料【補足②: 脆弱性診断】](#)へ

脆弱性診断						
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック (記入不要)	グローバルIPアドレス 設定機器
診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に問題ございません。	機器A
診断希望あり	インターネット	固定IP	111.111.111.111	/32	記載に問題ございません。	機器A
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。			機器B
	閉域網					

脆弱性診断関連の情報の記入④

4. 回線情報シートの作成

脆弱性診断関連の情報を記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

■ 固定IP/動的IP

グローバルIPアドレスが変動しない場合は「固定IP」を、変動する場合は「動的IP」を、プルダウンメニューよりお選びください。

※固定IP/動的IPの確認方法について、

7. 追加説明資料【補足④: 固定IP/動的IP確認方法】をご参照ください。

■ 固定IPを選んだ場合

⇒[【脆弱性診断関連の情報の記入⑤】](#)へ

■ 動的IPを選んだ場合

⇒[【脆弱性診断関連の情報の記入⑥】](#)へ

⇒以下2点の両方に該当する場合、脆弱性診断の実施日にグローバルIPアドレスを確認の上、ご記入していただく必要があります。

- 「脆弱性診断希望」にて「調査希望あり」を選択した場合
- 「固定IP/動的IP」にて「動的IP」を選択した場合

※詳しい記入方法については、

7. 追加説明資料【補足⑧: 脆弱性診断当日の流れ】をご参照ください。

脆弱性調査
調査希望ありの場合

脆弱性診断						
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック (記入不要)	グローバルIPアドレス 設定機器
診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に問題ございません。	機器A
診断希望あり	インターネット	固定IP	111.111.111.111	/32	記載に問題ございません。	機器A
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。			機器B
	閉域網					

脆弱性診断関連の情報の記入⑤

4

脆弱性調査
調査希望ありの場合

脆弱性診断関連の情報を記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

「固定IP/動的IP」にて
「固定IP」を選んだ場合

■ グローバルIPアドレス

回線が使用しているグローバルIPアドレスをご記入ください。
動的グローバルIPアドレスである場合、脆弱性診断当日に連携をお願いいたします。

※動的グローバルIPアドレスを脆弱性診断当日にご連携いただくにあたり、注意事項がございます。
必ず7. 追加説明資料【補足⑧:脆弱性診断当日の流れ】をご参考ください。

■ プレフィックス長

記載いただいたグローバルIPアドレスのプレフィックス長を記入いただく欄です。
「/32」が初期入力値です。

※詳細は7. 追加説明資料【補足⑤:プレフィックス長】をご参考ください。

■ 入力チェック

入力いただいたグローバルIPアドレスについて、脆弱性診断可能なグローバルIPアドレスか否かを確認する欄です。
新たに何かを記入いただく必要はございません。

※入力チェック欄に表示される値についての詳細は、
7. 追加説明資料【補足⑥:入力チェック】をご参照ください。

※脆弱性診断可能なIPアドレスについての詳細は、
7. 追加説明資料【補足⑦:脆弱性診断可能なIPアドレス】をご参照ください。

脆弱性診断						
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック (記入不要)	グローバルIPアドレス 設定機器
診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に問題ございません。	機器A
診断希望あり	インターネット	固定IP	111.111.111.111	/32	記載に問題ございません。	機器A
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。			機器B
	閉域網					

脆弱性診断関連の情報の記入⑥

4. 回線情報シートの作成

脆弱性診断関連の情報をご記入いただきます。「2.回線情報」シートの【脆弱性診断】に該当します。

■ グローバルIPアドレス設定機器

調査対象のグローバルIPアドレスが設定されている機器をお選びください。

※【回線に紐づく機器情報の記入】以降で機器情報をご記入いただき、「機器A」もしくは「機器B」を
プルダウンメニューよりお選びください。
詳細は【回線に紐づく機器情報の記入】以降をご参照ください。

脆弱性調査
調査希望ありの場合

脆弱性診断						
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック (記入不要)	
診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に問題ございません。	グローバルIPアドレス 設定機器 機器A
診断希望あり	インターネット	固定IP	111.111.111.111	/32	記載に問題ございません。	機器A
診断希望あり	インターネットVPN	動的IP	脆弱性診断当日に連携してください。			機器B
	閉域網					

回線に紐づく機器情報の記入①

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。
「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。
ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

■ 機器Aの記入方法について

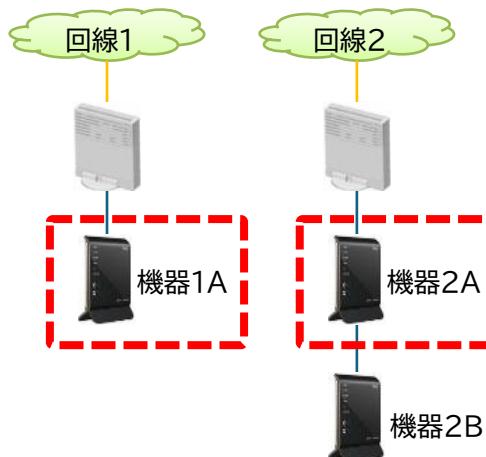
「機器A」について、【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器(最大2台)のうち、より回線終端装置に近いものをご記入ください。

※「機器B」について、機器Aに紐づいて存在している場合(機器Aの配下に機器Bがある場合)のみ、情報を記入いただきます。

■ 同一回線内で、ネットワーク機器を並列で使用している場合

同一回線内で、ネットワーク機器を並列で使用している場合、並列のうちの片方の機器については別の行を使用してご記載ください。
⇒ 詳細については、7. 追加説明資料【補足⑨:同一機器】をご参照ください。

機器Aの構成パターン(例)



機器A (ルータ/ファイアウォール/UTM)						
申告機器No. (ルータ/ ファイアウォール/ UTM)	機器種別	メーカー	型番	シリアルナンバー	同一機器 (他回線で同一機器があった場合、 申告機器No.を記入)	ファームウェアバージョン
例A	ルータ	シスコシステムズ	ISR 921	ABC123456SN	2A	15.1S
1A	ルータ	ヤマハ	RTX830	1234567899		15.02.31
2A	ファイアウォール/UTM	フォーティネット	FortiGate 40F	5555AAAAA		7.2
3A	ルータ	シスコシステムズ	ISR 921	123ABC456		15.1S

回線に紐づく機器情報の記入②

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。
「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。
ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

■ 申告機器No.

ご申告いただく機器について、番号を付与する欄です。
新たに何かをご記入いただく必要はございません。
※現地調査時や、調査報告書等で使用いたしますため、
医療機関様にて変更いただかないようお願ひいたします。

■ 機器種別

「ルータ」「ファイアウォール/UTM」のうち、使用しているものを
プルダウンメニューより選択してください。

■ メーカー

「機器種別」の選択内容に対応したメーカーをご記入ください。
プルダウンメニューより選択いただくことも可能です。

■ 型番

該当機器の「型番」をご記入ください。
※「製品名」や「シリーズ名」についても、「型番」欄の中に併せて
ご記載ください。
例) ヤマハの場合⇒「RTX830」
シスコシステムズの場合⇒「Cisco Firepower 1000」

機器A(ルータ/ファイアウォール/UTM)							
申告機器No. (ルータ/ ファイアウォール/ UTM)	機器種別	メーカー	型番	シリアルナンバー	同一機器 (他回線で同一機器があった場合、 申告機器No.を記入)	ファームウェアバージョン	機器設置場所
例A	ルータ	シスコシステムズ	ISR 921	ABC123456SN	2A	15.1S	本部棟 3F サーバー室 1番ラック 7U
1A	ルータ	ヤマハ	RTX830	1234567899		15.02.31	1F サーバ室
2A	ファイアウォール/UTM	フォーティネット	FortiGate 40F	5555AAAAA		7.2	1F サーバ室
3A	ルータ	シスコシステムズ	ISR 921	123ABC456		15.1S	1F サーバ室

回線に紐づく機器情報の記入③

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。

「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。

ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

■ シリアルナンバー

該当機器のシリアルナンバーをご記入ください。

※多くの機器には、本体の側面、背面、底面にシリアルナンバーが記載されたラベル・ステッカーがございます。

ラベルには「Serial Number」や「S/N」という表記とともに、番号が記載しております。

これらをご確認いただき、正確にご記入ください。

■ 同一機器

同じ機器が他の回線にも接続されており、他の回線に記載されている場合、その機器の「申告機器No.」をご記入ください。

※詳細は7. 追加説明資料【補足⑨:同一機器】をご参照ください。

機器A (ルータ/ファイアウォール/UTM)							
申告機器No. (ルータ/ ファイアウォール/ UTM)	機器種別	メーカー	型番	シリアルナンバー	同一機器 (他回線で同一機器があった場合、 申告機器No.を記入)	ファームウェアバージョン	機器設置場所
例A	ルータ	シスコシステムズ	ISR 921	ABC123456SN	2A	15.1S	本部棟 3F サーバー室 1番ラック 7U
1A	ルータ	ヤマハ	RTX830	1234567899		15.02.31	1F サーバ室
2A	ファイアウォール/UTM	フォーティネット	FortiGate 40F	5555AAAAA		7.2	1F サーバ室
3A	ルータ	シスコシステムズ	ISR 921	123ABC456		15.1S	1F サーバ室

回線に紐づく機器情報の記入④

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。
「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。
ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

■ ファームウェアバージョン

機器に対応したファームウェアバージョンをご記入ください。

システム的に自動更新となっている場合、該当の欄には「自動更新」とご記入ください。

詳細については、システムベンダ様にご確認をお願いいたします。

主要なメーカーの装置に関しては、確認手順書を準備しておりますので、ポータルシステムをご参照ください。

■ 機器設置場所

機器が設置されている部屋やラック位置をご記入ください。

棟や階数、部屋名、ラックに設置されている場合は、ラック番号、ユニット番号など、できるだけ詳しい設置場所をご記入ください。

詳細な設置場所をご記入いただくことで、当日の作業がスムーズになります。

ご協力をお願いします。

機器A (ルータ/ファイアウォール/UTM)							
申告機器No. (ルータ/ ファイアウォール/ UTM)	機器種別	メーカー	型番	シリアルナンバー	同一機器 (他回線で同一機器があった場合、 申告機器No.を記入)	ファームウェアバージョン	機器設置場所
例A	ルータ	シスコシステムズ	ISR 921	ABC123456SN	2A	15.1S	本部棟 3F サーバー室 1番ラック 7U
1A	ルータ	ヤマハ	RTX830	1234567899		15.02.31	1F サーバ室
2A	ファイアウォール/UTM	フォーティネット	FortiGate 40F	5555AAAAA		7.2	1F サーバ室
3A	ルータ	シスコシステムズ	ISR 921	123ABC456		15.1S	1F サーバ室

回線に紐づく機器情報の記入⑤

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。
「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。
ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

- 桁数**
使用しているパスワードの桁数について、「8桁未満」、「8~12桁」、「13桁以上」、「把握していない」のいずれかを、プルダウンメニューよりお選びください。

- 文字混在(英数字、記号)**
使用しているパスワードで英数字と記号を組み合わせているか、「混在あり」、「混在なし」、「把握していない」からお選びください。

- 推測困難な文字列**
使用しているパスワードを知らない人でも推測できるパスワードを使用しているか、「はい」、「いいえ」、「把握していない」からお選びください。
※ログインIDと同一である場合や、既存の単語1語のみである場合などは、推測が容易な文字列といえます。

- ✓ 適切なパスワード管理がサイバーセキュリティ対策につながるため、「パスワードポリシー確認」を実施いたします。
- ✓ 本事業の回答内容・調査結果について、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。

アカウント・パスワードを医療機関様側で管理していない場合、該当機器を管理しているベンダ様へお問い合わせください。

M) 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	定期的な変更	工場出荷時の設定から 変更している	必要な権限に応じて アカウントを分けている	他の機器やアカウントと 異なるパスワードを使用している
13桁以上	混在あり	はい	なし	はい	分けている	はい

回線に紐づく機器情報の記入⑥

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。

「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。

ネットワーク機器が2台ある場合、より回線終端装置に近いほうを「機器A」としてご記載ください。

■ 定期的な変更

使用しているパスワードを変更しているかについて、「2ヶ月以内」、「3~6ヶ月以内」、「7ヶ月~1年未満」、「1年以上」、「不定期」、「把握していない」より、あてはまる期間をお選びください。

■ 工場出荷時の設定から変更している

パスワードを工場出荷時から変更し独自のパスワードにしているか、「はい」、「工場出荷時のパスワードを使用している」、「把握していない」よりお選びください。

■ 必要な権限に応じてアカウントを分けている

権限ごとにアカウントを分けているか、「分けている」、「分けていない」、「把握していない」からお選びください。

■ 他の機器/アカウントと異なるパスワードを使用している

使用しているパスワードと同一のパスワードを他の機器でも使用しているか、「はい」、「いいえ」、「把握していない」からお選びください。

✓ 適切なパスワード管理がサイバーセキュリティ対策につながるため、「パスワードポリシー確認」を実施いたします。

✓ 本事業の回答内容・調査結果について、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。

アカウント・パスワードを医療機関様側で管理していない場合、該当機器を管理しているベンダ様へお問い合わせください。

M)						
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	定期的な変更	工場出荷時の設定から 変更している	必要な権限に応じて アカウントを分けている	他の機器やアカウントと 異なるパスワードを使用している
13桁以上	混在あり	はい	なし	はい	分けている	はい

回線に紐づく機器情報の記入⑦

4. 回線情報シートの作成

【回線情報】欄にて記入いただいたインターネット回線に紐づいているネットワーク機器を、「機器A」「機器B」として最大2台記入いただきます。
「2.回線情報」シートの【機器A(ルータ/ファイアウォール/UTM)】【機器B(ルータ/ファイアウォール/UTM)】に該当します。
「機器A」を記載した回線に、さらにネットワーク機器が存在する場合、「機器B」をご記入ください。

■ 機器Bの記入条件について

「機器B」について、機器Aに紐づいて存在している場合(機器Aの配下に機器Bがある場合(※1))のみ、情報をご記入ください。
同一回線内で、ネットワーク機器を並列で使用していた場合、並列の機器については別の行を使用してご記載ください。
⇒ 7. 追加説明資料【補足⑨:同一機器】をご参考ください。

■ 機器Bの記入方法について

「機器B」の記入方法は、「機器A」の記入方法と同様です。
【回線に紐づく機器情報の記入①～⑥】をご参考ください。

※1 機器Bがある場合の構成イメージ



機器B (ルータ/ファイアウォール/UTM)							
申告機器No. (ルータ/ ファイアウォール/ UTM)	機器種別	メーカー	型番	シリアルナンバー	同一機器 (他回線で同一機器があった場合、 申告機器No.を記入)	ファームウェアバージョン	機器設置場所
例A	ルータ	シスコシステムズ	ISR 921	ABC123456SN	2A	15.1S	本部棟 3F サーバ室 1番ラック 7U
1A	ルータ	ヤマハ	RTX830	1234567899		15.02.31	1F サーバ室
2A	ファイアウォール/UTM	フォーティネット	FortiGate 40F	5555AAAAA		7.2	1F サーバ室
3A	ルータ	シスコシステムズ	ISR 921	123ABC456		15.1S	1F サーバ室



5. 端末情報シートの作成



端末情報シートのヒアリング内容

4. 端末情報シートの作成

- 端末情報シートでは、以下の内容をヒアリングさせていただきます。

- 端末についての基本情報
- 電子カルテサーバー、端末のパスワードポリシー
- ウィルス対策の有無
- WindowsUpdate有無

基本情報シート	回線情報シート	端末情報シート	設置場所情報シート
<p>基本情報の記入 医療機関名、メイン担当者・立会者情報などを記入する。</p> <p>脆弱性診断関連の情報の記入 脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。</p>	<p>回線についての基本情報の記入 洗い出した回線情報を記入する。</p> <p>回線に紐づく機器情報の記入 記入した回線に紐づくネットワーク機器の情報を記入する。</p> <p>各機器におけるパスワードポリシーの記入 記入した機器におけるパスワードポリシーを記入する。</p>	<p>端末についての基本情報の記入 電子カルテ・医療情報システムで使用している端末情報を記入する。</p> <p>セキュリティ対策状況・パスワードポリシーの記入 記入した端末におけるセキュリティ対策状況、パスワードポリシーを記入する。</p>	<p>機器の設置場所を示す平面図の作成 回線情報シート、端末情報シートにて記入した機器の設置場所を平面図上にあらわす。</p>

端末についての基本情報の記入①

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの「端末情報」に該当します。

■ 申告端末No.

ご申告いただく端末(以降、「調査端末」と表記)について、番号を付与する欄です。

新たに何かをご記入いただく必要はございません。

※現地調査時や、調査報告書等で使用いたしますため、医療機関様にて変更いただかないようお願いいたします。

■ システム種別

調査端末が利用している医療情報システムについて、「電子カルテ」「放射線検査」「その他検査」「薬剤」「看護」「医事会計」「上記以外のシステム」よりお選びください。

■ シンクライアント利用

調査端末がシンクライアント端末(シンクラ)である場合、「はい」を、そうではない場合は「いいえ」をお選びください。

※シンクライアント端末(シンクラ)とは、クライアント側の端末(PC)では限られた処理しか行わず、

アプリケーションの実行やデータの管理など、ほとんどの処理をサーバ側(仮想デスクトップ)で行う仕組みのことです。

申告端末 No.	システム種別	シンクライアント利用	端末情報					
			シンクライアント/FAT端末		仮想デスクトップ	Windows OS/バージョン	ウイルス対策ソフト	
例	薬剤	いいえ	端末ホスト名	設置場所	端末導入時期			
サーバ	電子カルテ		PC×××	2F ○○室	2025年4月	PC×××	Windows 11	Windows Defender
※サーバについて、現地調査は実施せず、アカウント・パスワードポリシーの確認のみ行います。								
1	電子カルテ	はい	HOST	3F サーバ室	2025年7月1日	VHOST	Windows 11	Windows Defender
2	放射線検査	いいえ	HOST2	3F サーバ室	2023年2月1日		Windows 10	ESET HOME セキュリティ
3	その他検査	わからない	KANRI	3F サーバ室	2025年4月1日		Windows 11	ウイルスバスター クラウド
4	薬剤	いいえ	YAKUZAI	3F サーバ室	2025年4月1日		Windows 10	Trend Micro Apex One
5								

端末についての基本情報の記入②

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの「端末情報」に該当します。

■ シンクライアント/FAT端末/端末ホスト名

調査端末のホスト名(端末名)をご記入ください。

※実際に操作されている物理端末(シンクライアント端末や

FAT端末等)のホスト名をご記入ください。

仮想デスクトップのホスト名ではありませんのでご注意ください。

シンクライアント利用 ありの場合

■ 仮想デスクトップ/端末ホスト名

調査端末における仮想デスクトップのホスト名(端末名)をご記入ください。

■ 設置場所

調査端末が設置されている場所をご記入ください。

棟や階数、部屋名、ラックに設置されている場合は、

ラック番号、ユニット番号など、可能な限り詳しい設置場所をご記入ください。

詳細な設置場所をご記入いただくことで、当日の作業がスムーズになります。

ご協力をお願いします。

■ 端末導入時期

調査端末の導入時期をご記入ください。

※過去に調査端末を導入した際のおおよその時期をご記入ください

申告端末 No.	システム種別	シンクライアント利用	端末情報				Windows OS/バージョン	ウイルス対策ソフト
			端末ホスト名	設置場所	端末導入時期	端末ホスト名		
例	薬剤	いいえ	PCxxxx	2F OOO室	2025年4月	PCxxxx	Windows 11	Windows Defender
サーバ	電子カルテ						※サーバについて、現地調査は実施せず、アカウント・パスワードポリシーの確認のみ行います。	
1	電子カルテ	はい	HOST	3F サーバ室	2025年7月1日	VHOST	Windows 11	Windows Defender
2	放射線検査	いいえ	HOST2	3F サーバ室	2023年2月1日		Windows 10	ESET HOME セキュリティ
3	その他検査	わからない	KANRI	3F サーバ室	2025年4月1日		Windows 11	ウイルスバスター クラウド
4	薬剤	いいえ	YAKUZAI	3F サーバ室	2025年4月1日		Windows 10	Trend Micro Apex One
5								

端末についての基本情報の記入③

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの「端末情報」に該当します。

■ WindowsOSバージョン

調査端末のWindowsOSバージョンについて、「Windows10」「Windows11」のどちらかを
プルダウンメニューよりお選びください。

※現地調査について、基本的にWindowsOSはWindows10、11が対象となります。

※Windows7については、現地調査は可能ですが、一部調査できない項目がございます。

■ ウイルス対策ソフト

調査端末にインストールされているウイルス対策ソフトの製品名について、プルダウンメニュー(以下)より1つお選びください。
当てはまらない場合は、その製品名をご記入ください。

- ・Windows Defender
- ・ESET HOME セキュリティ
- ・Trend Micro Apex One
- ・ウイルスバスタークラウド
- ・ウイルスバスター タルセキュリティ
- ・Symantec Endpoint Protection
- ・ウイルス対策ソフト未導入

申告端末 No.	システム種別	端末情報						Windows OS/バージョン	ウイルス対策ソフト
		シンクライアント利用	端末ホスト名	設置場所	端末導入時期	端末ホスト名			
例	薬剤	いいえ	PC×××	2F ○○室	2025年4月	PC×××	Windows 11	Windows Defender	
※サーバについて、現地調査は実施せず、アカウント・パスワードポリシーの確認のみ行います。									
1	電子カルテ	はい	HOST	3F サーバ室	2025年7月1日	VHOST	Windows 11	Windows Defender	
2	放射線検査	いいえ	HOST2	3F サーバ室	2023年2月1日		Windows 10	ESET HOME セキュリティ	
3	その他検査	わからない	KANRI	3F サーバ室	2025年4月1日		Windows 11	ウイルスバスター クラウド	
4	薬剤	いいえ	YAKUZAI	3F サーバ室	2025年4月1日		Windows 10	Trend Micro Apex One	
5									

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの「USB使用制限」に該当します。

■ 制御の実施

USBの使用について、制御・制限している場合(USBポート無効化、ポートの閉塞等)には「実施あり」、していない場合には「実施なし」をプルダウンメニューよりお選びください。

※USBメモリなどの外部媒体を経由してランサムウェア等のマルウェアの侵入を許す場合があるため、
安易にUSB端子を利用できないように制限をかけることで、セキュリティを強化することができます。

✓ 本事業の回答内容・調査結果について、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ございません。

■ 制御手段

USBの使用を制御・制限している場合は、その手段をプルダウンメニュー(以下)より1つお選びください。
当てはまらない場合は、その手段の名称をご記入ください。

- ・SKYSEA Client View
- ・AssetView
- ・Microsoft Defender for Endpoint
- ・LB USBロック
- ・USBブロッカー
- ・端末レジストリ設定で制御
- ・ウイルス対策ソフトの一部機能で実施

USB使用制限		パスワードポリシー確認						
制御の実施	制御手段	桁数	文字混在 (英数字、記号)	推測困難な文 字列	定期的な変更	必要な権限に応じて アカウントを分けている	他の機器/アカウントと 異なるパスワードを使用している	二要素認証
実施あり	グループポリシー(ADサーバ)で制御	13桁以上	混在あり	いいえ	3~6ヶ月以内	分けている	いいえ	実施している
把握していない		13桁以上	混在あり	把握していない	なし	分けている	はい	把握していない
		8~12桁	混在なし	いいえ	2ヶ月以内	分けていない	いいえ	実施していない

セキュリティ対策状況・パスワードポリシーの記入②

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【パスワードポリシー確認】に該当します。
すべてプルダウンメニューより選択いただくものとなります。

■ 行数

使用しているパスワードの行数について、「8行未満」、「8~12行」、「13行以上」、「把握していない」からお選びください。

■ 文字混在(英数字、記号)

使用しているパスワードで英数字や記号を組み合わせているか、「混在あり」、「混在なし」、「把握していない」からお選びください。

■ 推測困難な文字列

使用しているパスワードを知らない人でも推測できるパスワードを使用しているか、「はい」、「いいえ」、「把握していない」からお選びください。

ログインIDと同一である場合や、既存の単語1語のみである場合などが、推測が容易な文字列として挙げられます。

パスワードポリシーのみ
電子カルテシステムのサーバについてもご回答ください

- ✓ 適切なパスワード管理がサイバーセキュリティ対策につながるため、「パスワードポリシー確認」を実施いたします。
- ✓ 本事業の回答内容・調査結果について、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。

USB使用制限					パスワードポリシー確認			
制御の実施	制御手段	行数	文字混在(英数字、記号)	推測困難な文字列	定期的な変更	必要な権限に応じてアカウントを分けている	他の機器/アカウントと異なるパスワードを使用している	二要素認証
実施あり	グループポリシー(ADサーバ)で制御	13行以上	混在あり	いいえ	3~6か月以内	分けている	いいえ	実施している
		13行以上	混在あり	把握していない	なし	分けている	はい	把握していない
把握していない		8~12行	混在なし	いいえ	2か月以内	分けていない	いいえ	実施していない

セキュリティ対策状況・パスワードポリシーの記入③

5. 端末情報シート の作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【パスワードポリシー確認】に該当します。
すべてプルダウンメニューより選択いただくものとなります。

■ 定期的な変更

使用しているパスワードを変更しているかをご記入ください。

変更している場合には、

「2か月以内」、「3~6か月以内」、「7か月~1年未満」、「1年以上」、
「不定期」、「把握していない」から、あてはまる期間をお選びください。

■ 必要な権限に応じてアカウントを分けている

権限ごとにアカウントを分けているか、

「分けている」、「分けていない」、「把握していない」からお選びください。

■ 他の機器/アカウントと異なるパスワードを使用している

使用しているパスワードと同一のパスワードを他の機器でも使用しているか、
「はい」、「いいえ」、「把握していない」からお選びください。

■ 二要素認証

二要素認証を実施しているか、
「実施している」、「実施していない」、
「把握していない」からお選びください。

※詳細については、

7. 追加説明資料【補足⑩:二要素認証】
をご参照ください。

パスワードポリシーのみ
電子カルテシステムのサーバに
についてもご回答ください

- ✓ 適切なパスワード管理がサイバーセキュリティ対策につながるため、「パスワードポリシー確認」を実施いたします。
- ✓ 本事業の回答内容・調査結果について、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。

USB使用制限					パスワードポリシー確認			
制御の実施	制御手段	桁数	文字混在 (英数字、記号)	推測困難な文字列	定期的な変更	必要な権限に応じて アカウントを分けている	他の機器/アカウントと 異なるパスワードを使用している	二要素認証
実施あり	グループポリシー(ADサーバ)で制御	13桁以上	混在あり	いいえ	3~6か月以内	分けている	いいえ	実施している
		13桁以上	混在あり	把握していない	なし	分けている	はい	把握していない
把握していない		8~12桁	混在なし	いいえ	2か月以内	分けていない	いいえ	実施していない

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【WindowsUpdate】に該当します。

■ WindowsUpdate実施状況

調査端末におけるWindowsUpdateの実施有無について、「実施している」、「実施していない」、「把握していない」からお選びください。

※「実施している」を選択すると「実施している場合」の記入欄が、「実施していない」「把握していない」を選択すると「実施していない場合」の記入欄が黄色く表示されます。

■ 「実施している」を選択した場合

⇒【セキュリティ対策状況・パスワードポリシーの記入⑥】へ

■ 「実施していない」「把握していない」を選択した場合

⇒【セキュリティ対策状況・パスワードポリシーの記入⑦⑧】へ

✓ 本事業の回答内容・調査結果について、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。

WindowsUpdate 実施状況	WindowsUpdate			
	実施している場合	実施していない/把握していない理由	実施していない/把握していない場合	端末を管理している事業者（ベンダ）名 (自由記述)
実施している	WindowsUpdateの適用頻度 1か月以下をひとつの周期として定めている。その周期に従い適用している。	実施していない/把握していない理由 アップデート後のWindowsバージョンでは動作保証ができないため	実施している	○○ベンダ
実施している	1か月以内をひとつの周期として定めている。その周期に従い適用している。			
実施していない		アップデートの必要性を感じていないため		

セキュリティ対策状況・パスワードポリシーの記入⑤

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【WindowsUpdate】に該当します。

■ WindowsUpdateの適用頻度

WindowsUpdateの適用頻度について、プルダウンメニュー(以下)より1つお選びください。

- ・Windows更新プログラムが配布され次第すぐに適用している。
- ・1ヶ月以内をひとつの周期として定めている。その周期に従い適用している。
- ・2~3ヶ月をひとつの周期として定めている。その周期に従い適用している。
- ・4~6ヶ月をひとつの周期として定めている。その周期に従い適用している。
- ・7ヶ月~1年未満の期間をひとつの周期として定めている。その周期に従い適用している。
- ・1年以上の期間をひとつの周期として定めている。その周期に従い適用している。
- ・期間に依らない特定のルール・ポリシーがあり、端末導入後に適用実績がある。
- ・期間に依らない特定のルール・ポリシーはないが、端末導入後に適用実績がある。

WindowsUpdateを
「実施している」場合

- ✓ 本事業の回答内容・調査結果について、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ございません。

WindowsUpdate 実施状況	WindowsUpdate			
	実施している場合	実施していない場合	実施していない/把握していない場合	端末を管理している事業者（ベンダ）名 (自由記述)
実施している	WindowsUpdateの適用頻度 1ヶ月以下をひとつの周期として定めている。その周期に従い適用している。	実施していない/把握していない理由 アップデート後のWindowsバージョンでは動作保証ができないため	実施している	○○ベンダ
実施している	1ヶ月以内をひとつの周期として定めている。その周期に従い適用している。			
実施していない		アップデートの必要性を感じていないため		

セキュリティ対策状況・パスワードポリシーの記入⑥

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【WindowsUpdate】に該当します。

■ 実施していない/把握していない理由

WindowsUpdateを実施していない・把握していない理由について、プルダウンメニュー(以下)より1つお選びください。

- ・アップデート後のWindowsバージョンでは動作保証ができないため
- ・アップデートのためにシステムを停止させることができないため
- ・アップデートの必要性を感じていないため
- ・費用的に困難なため
- ・事業者(ベンダ)が対応しないため
- ・インターネットに接続させないクローズド・ネットワークにより運用しているため
- ・その他

WindowsUpdateを「実施していない/把握していない」場合

- ✓ 本事業の回答内容・調査結果について、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ございません。

WindowsUpdate 実施状況	実施している場合		WindowsUpdate		実施していない/把握していない場合
	WindowsUpdateの適用頻度	実施していない/把握していない理由	医療情報システムにおける、アップデートに影響の出るようなカスタマイズの実施	端末を管理している事業者(ベンダ)名 (自由記述)	
実施している	1か月以下をひとつの周期として定めている。その周期に従い適用している。	アップデート後のWindowsバージョンでは動作保証ができないため	実施している	○○ベンダ	
実施している	1か月以内をひとつの周期として定めている。その周期に従い適用している。				
実施していない		アップデートの必要性を感じていないため			

セキュリティ対策状況・パスワードポリシーの記入⑦

5. 端末情報シートの作成

調査端末(最大5台)の基本情報をご記入いただきます。「3.端末情報」シートの【WindowsUpdate】に該当します。
※「備考」欄に関しては、【WindowsUpdate】のみでなく、端末情報すべてにおいて留意事項があればご記入ください。

■ 医療情報システムにおける、アップデートに影響の出るようなカスタマイズの実施有無

調査端末について、接続している医療情報システムに、WindowsUpdateの実施に影響が出るようなカスタマイズを実施しているかどうか、「実施している」「実施していない」「把握していない」のいずれかを、プルダウンメニューよりお選びください。

WindowsUpdateを
「実施していない/
把握していない」場合

■ 端末を管理している事業者(ベンダ)

調査端末を管理している事業者(ベンダ)名について、記入欄にご記入ください。

✓ 本事業の回答内容・調査結果について、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ございません。

■ 備考

現地調査を実施するにあたり、留意事項がございましたら、その内容をご記入ください。

WindowsUpdate		実施していない/把握していない場合		備考
実施していない/把握していない理由	医療情報システムにおける、アップデートに影響の出るようなカスタマイズの実施	端末を管理している事業者(ベンダ)名(自由記述)		
アップデート後のWindowsバージョンでは動作保証ができないため	実施している	○○ベンダ		
アップデート後のWindowsバージョンでは動作保証ができないため	実施していない	Vendor		



6. 設置場所情報シートの作成



設置場所情報シートのヒアリング内容

6. 設置場所情報シートの作成

- 設置場所情報シートでは、以下の内容をヒアリングさせていただきます。

- 院内平面図(フロア図)の貼付
- 回線終端装置・機器AB・申告端末(調査端末)1~5の設置場所に吹き出しを配置

基本情報シート	回線情報シート	端末情報シート	設置場所情報シート
基本情報の記入 医療機関名、メイン担当者・立会者情報などを記入する。	回線についての基本情報の記入 洗い出した回線情報を記入する。	端末についての基本情報の記入 電子カルテ・医療情報システムで使用している端末情報を記入する。	機器の設置場所を示す平面図の作成 回線情報シート、端末情報シートにて記入した機器の設置場所を平面図上にあらわす。
脆弱性診断関連の情報の記入 脆弱性診断の実施希望有無、グローバルIPアドレスなどを記入する。	回線に紐づく機器情報の記入 記入した回線に紐づくネットワーク機器の情報を記入する。 各機器におけるパスワードポリシーの記入 記入した機器におけるパスワードポリシーを記入する。	セキュリティ対策状況・パスワードポリシーの記入 記入した端末におけるセキュリティ対策状況、パスワードポリシーを記入する。	

機器の設置場所を示す平面図の作成①

6. 設置場所情報 シートの作成

【回線情報】シートで記入いただいた回線終端装置・機器AB、【端末情報】シートにてご記入いただいた端末の設置場所を平面図上に示していただきます。
平面図の画像を貼り付け、平面図上にオブジェクトの配置をお願いいたします。

■ 平面図を貼付する

「平面図貼り付け」と記入されているセルをクリックし、選択します。

「挿入」タブをクリック

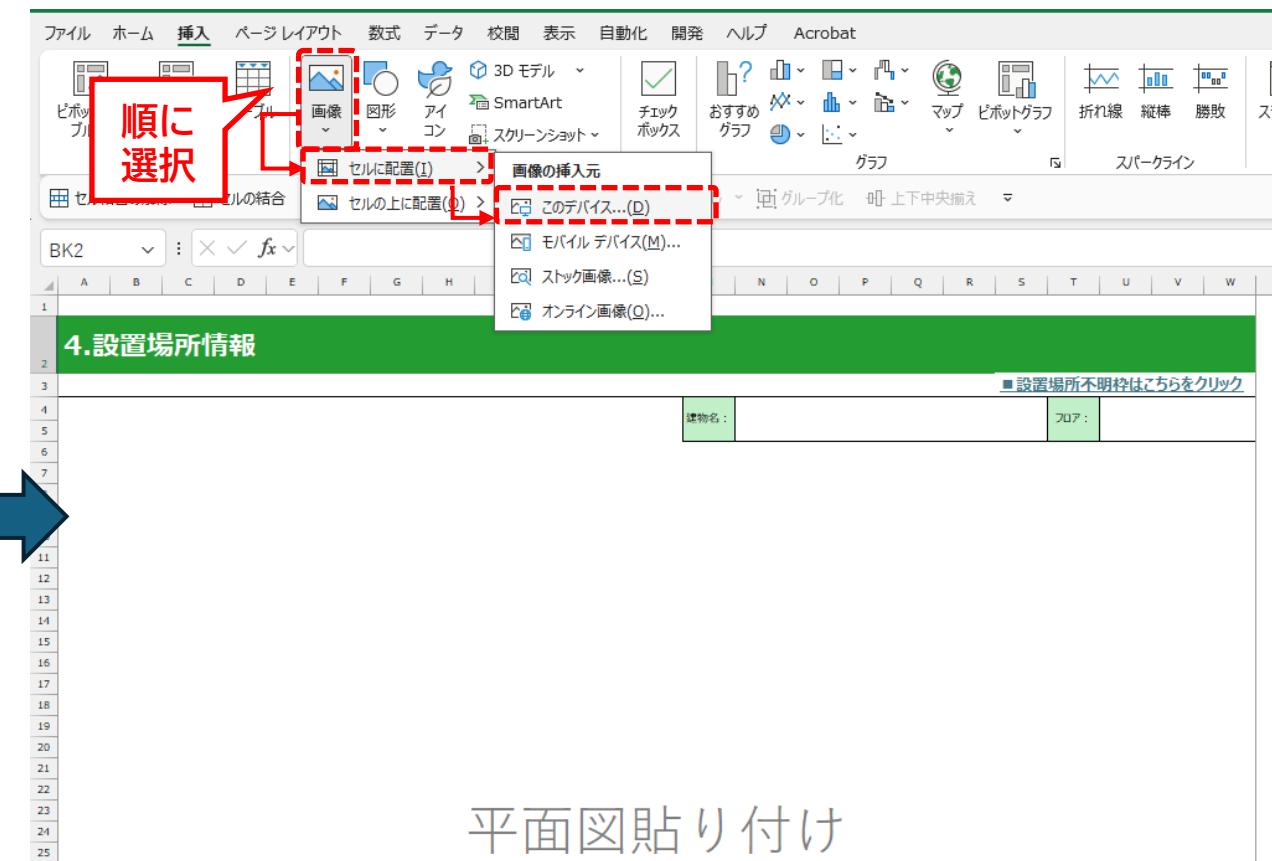
⇒「図」アイコンをクリック

⇒「画像」を選択

⇒「セルに配置」をクリック

⇒「このデバイス」を選択

⇒貼り付けたい平面図の画像を選び、貼り付けてください。



平面図貼り付け

機器の設置場所を示す平面図の作成②

6. 設置場所情報シートの作成

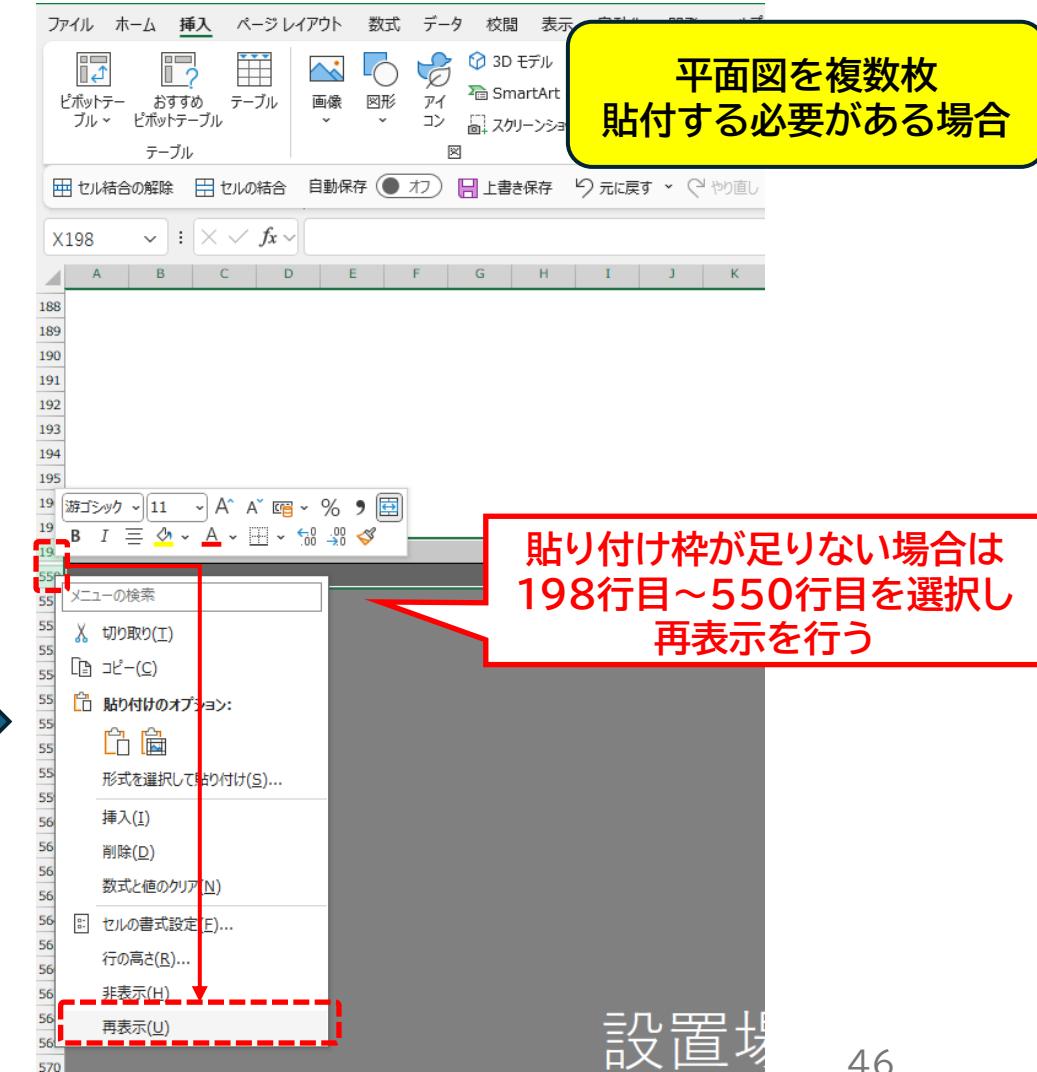
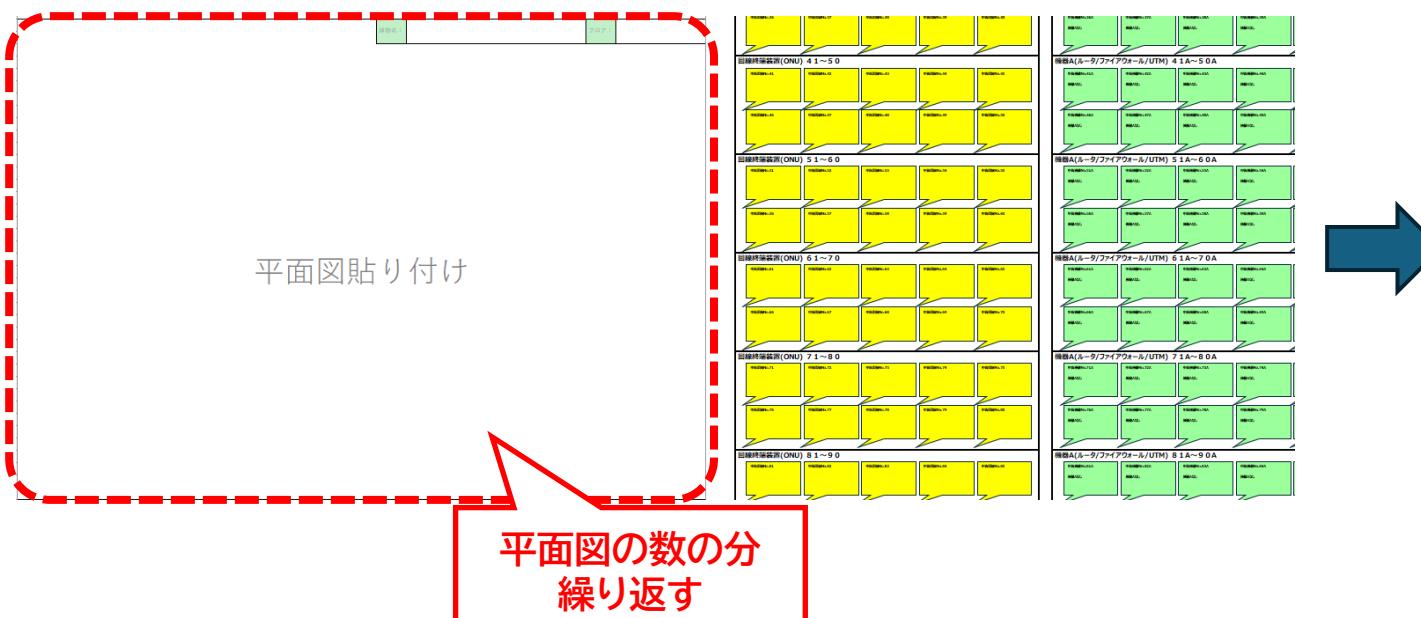
【回線情報】シートで記入いただいた回線終端装置・機器AB、【端末情報】シートにてご記入いただいた端末の設置場所を平面図上に示していただきます。平面図の画像を貼り付け、平面図上にオブジェクトの配置をお願いいたします。

■ 平面図画像を複数枚貼り付けたい場合

43行以降に用意されている貼り付け欄を選択し、必要な枚数文、貼り付け手順を繰り返してください。

■ 5枚以上貼り付けが必要な場合

5枚目と設置場所不明枠の間の198行目～550行目を選択し、マウスを右クリック
⇒再表示を選択し、貼り付け枠を増やしてください。



機器の設置場所を示す平面図の作成③

6. 設置場所情報シートの作成

【回線情報】シートで記入いただいた回線終端装置・機器AB、【端末情報】シートにてご記入いただいた端末の設置場所を平面図上に示していただきます。平面図の画像を貼り付け、平面図上にオブジェクトの配置をお願いいたします。設置場所が不明な場合は、「設置場所不明枠」への配置をお願いいたします。

■ 設置場所吹き出しを配置する

平面図画像を貼付いただいたのち、調査対象機器や調査対象端末の情報が入った吹き出しアイコンをクリックし、実際の設置場所にドラック＆ドロップして配置します。

端末(PC)、回線終端装置(ONU)の吹き出しアイコンは、必ず配置いただくようお願いします。

■ 吹き出しアイコンの形を調整する

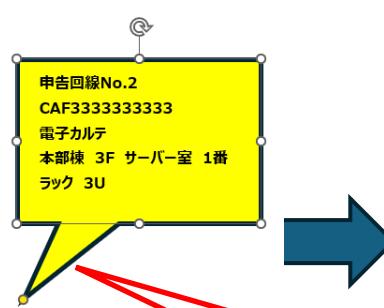
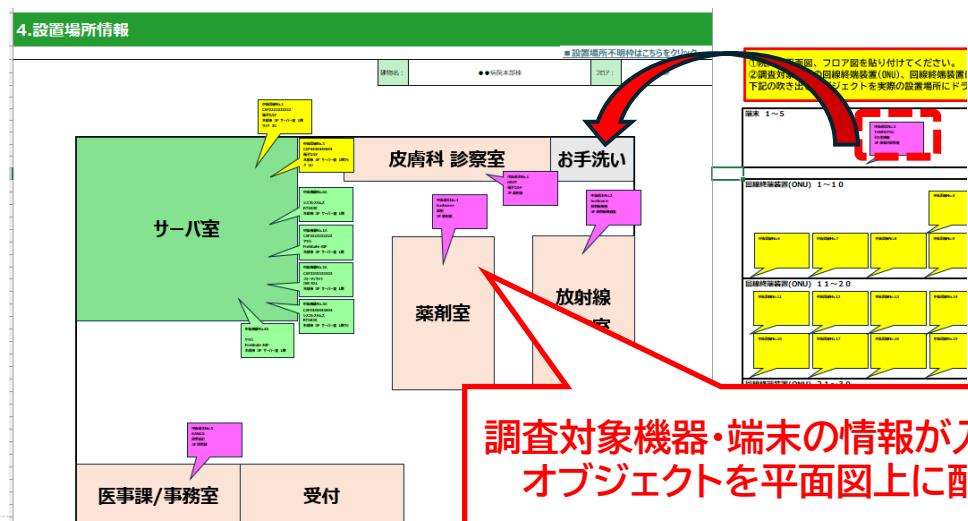
吹き出しアイコンをクリックして選択し、黄色の丸部分をドラッグすることで、吹き出しのしっぽの位置や長さを自由に調節することができます。長さを調節いただき、該当機器・端末の設置場所を可能な限り正確にお示しください。

■ 設置場所不明な機器・端末がある場合

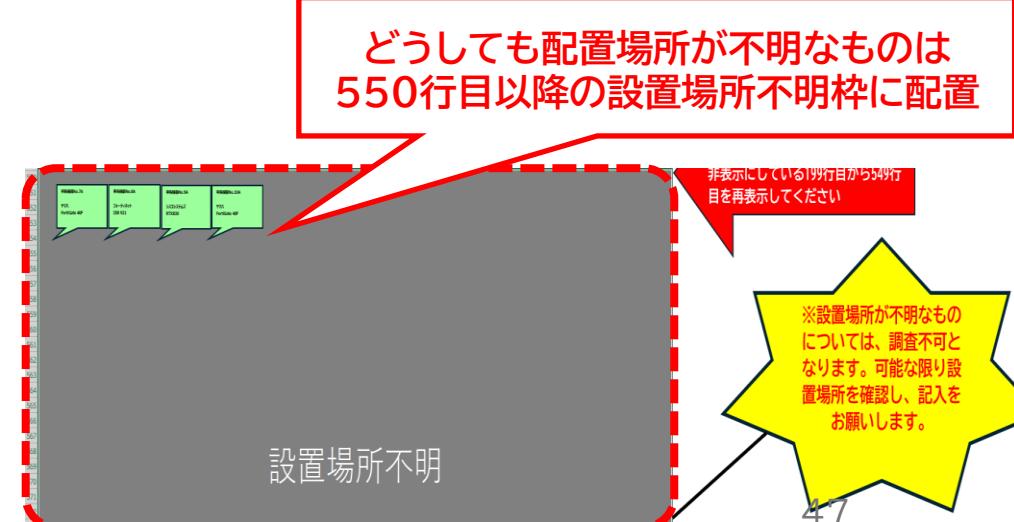
設置場所が不明な機器や端末がある場合は、画面下部にある「設置場所不明枠」に配置をお願いします。

※設置場所が不明な機器・端末については、現地調査不可となる可能性があります。

可能な限り設置場所を確認し、ご記入ください。



しっぽの長さを
調節





7. 追加說明資料



補足①:用途、システム名

■ 用途・システム名

該当する回線に紐づく医療情報システムについて、プルダウンメニューよりお選びください。

プルダウンメニューにある内容がどの用途、システムと結びつくかについて、以下の表に示しておりますため、ご参考ください。

関連スライド
:回線基本情報の記入①

No.	分類	カテゴリ(プルダウンメニュー)	該当する主な用途、システム・備考
1	医療情報システム	電子カルテシステム	電子カルテ ※保守用回線を含みます
2		部門システム	細菌/検体/放射線/病理/生理/給食/薬剤/看護支援/リハビリ支援/DWH/遠隔投影サービス(映像解析の外部委託)/健康診断 など ※保守用回線を含みます
3		医療事務・会計システム	医事会計/オンライン資格確認/オンライン請求 など ※保守用回線を含みます
4	医療機器	医療機器	PACS(放射線システム)/CT・MRI(画像系システム)/心電図/超音波/内視鏡など ※ネットワーク接続がある医療機器が対象となります ※保守用回線を含みます
5	地域医療連携システム	地域医療連携システム	地域医療連携システム ※保守用回線を含みます
6	院内ネットワーク	アップデート関連	WindowsUpdate用回線/セキュリティパッチ用回線/その他アップデート関連の回線 など
7	上記以外	上記以外	その他

補足②：脆弱性診断

7. 追加説明資料

■ 脆弱性診断について

グローバルIPアドレスを持つ機器に対して、遠隔地からリモート接続により脆弱性診断を実施いたします。

現地調査当日とは異なり、脆弱性診断当日の立ち合いは不要となります。

脆弱性診断の内容は、対象機器のグローバルIPアドレスに対してのポートスキャン(TCP/UDP)になります。

ポートスキャンの結果、ポートからの応答があった場合は、応答するポートに対して脆弱性スキャンを実施いたします。

脆弱性スキャンによって判明した、既知の脆弱性や設定の不備等によるセキュリティ上の問題点等については、調査報告書にてご報告させていただきます。

■ 脆弱性診断の対象について

リモートによる診断のため、インターネットとの通信が可能な機器が対象となります。

そのため、グローバルIPアドレスを持つ機器が診断可能です。

※グローバルIPアドレスを持たない機器は対象外

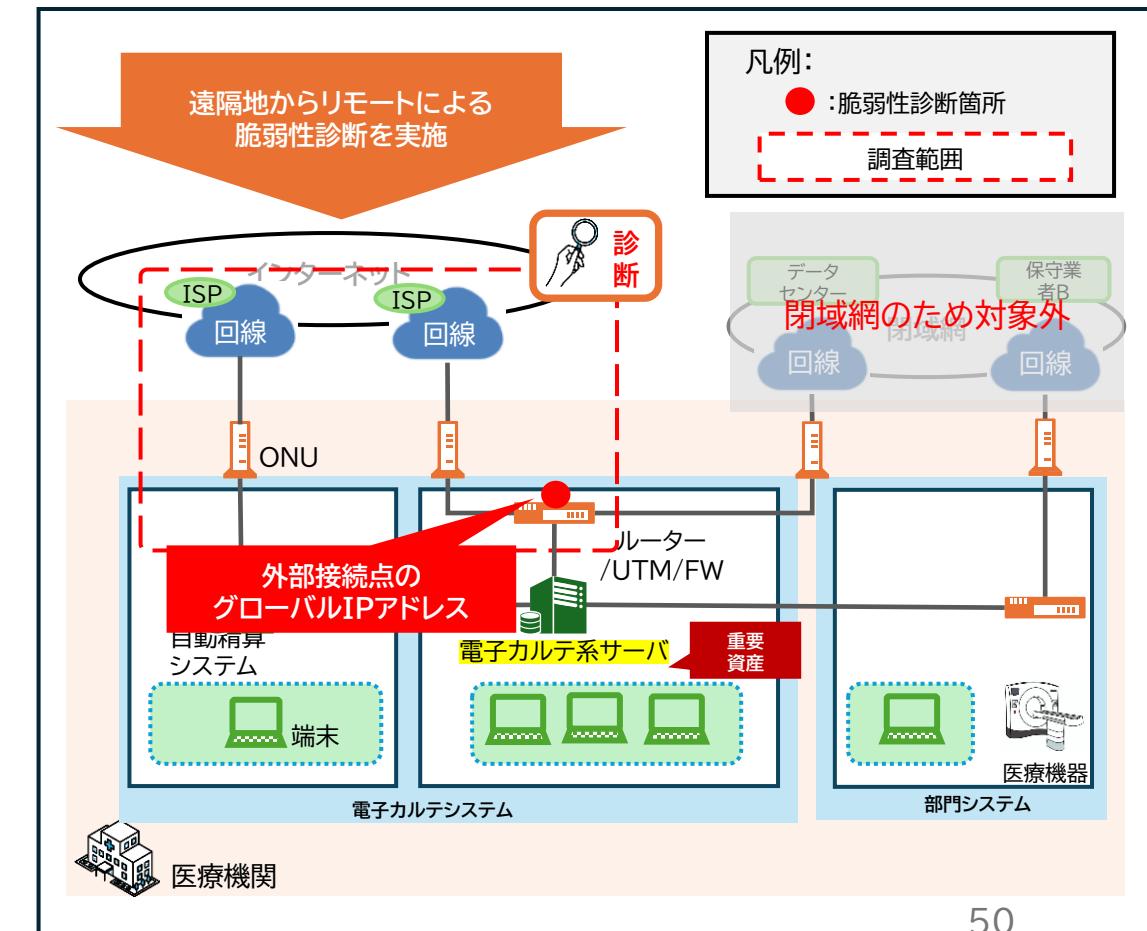
※脆弱性診断が実施可能な条件については、

7. 追加説明資料【補足③：通信形態】をご参照ください。

■ 脆弱性診断による業務影響について

脆弱性診断の実施による業務影響は発生しない想定です。

関連スライド
:脆弱性診断関連の情報の記入①



補足③:通信形態

■ インターネットと閉域網

- ・**インターネット** =不特定多数が利用可能な世界規模のネットワークを指します。
- ・**閉域網** =関係者のみが利用可能な、インターネットから切り離された独自のネットワークを指します。
主な種類: 専用線、IP-VPN、広域イーサネットなど

関連スライド
:脆弱性診断関連の情報の
記入②
:補足②:脆弱性診断

(※ネットワーク=複数のコンピューターが接続されているグループのこと)

■ インターネットVPNとIP-VPN

- ・**インターネットVPN**=インターネット内に、疑似的な専用の接続環境をつくる。
(インターネットVPNはインターネットを経由するため、必ずグローバルIPアドレスがございます。)
- ・**IP-VPN**=インターネットを経由せず、専用の接続環境をつくる。
(IP-VPNはインターネットを経由しないため、閉域網となり、グローバルIPアドレスはございません。)

- 各通信形態を選択した場合の記入パターンは以下になる想定です。回線情報記入シート作成の際、参考にしてください。

通信形態	固定IP/ 動的IP	グローバルIPアドレス		脆弱性診断 実施可否	備考
		ヒアリングシートへの グローバルIPアドレスの記入	脆弱性診断当日の グローバルIPアドレス連携要否		
インターネット	固定IP	必須	不要	○	
	動的IP	不要	必須	○	脆弱性診断当日の午前11時までにグローバルIPアドレスの連携がない場合、脆弱性診断の実施はできません。
インターネット VPN	固定IP	必須	不要	○	
	動的IP	不要	必須	○	脆弱性診断当日の午前11時までにグローバルIPアドレスの連携がない場合、脆弱性診断の実施はできません。
閉域網	-	-	-	×	

グローバルIPアドレスについては、システムベンダ様にご確認をお願いいたします。
※以下に記載の確認方法につきまして、医療機関様側で確認が必要になった場合にご参照ください。

関連スライド
:脆弱性診断関連の情報の
記入③

- グローバルIPアドレスが固定IPアドレスか動的IPアドレスかを確認する方法について
使用しているグローバルIPアドレスが「固定IPアドレス」か「動的IPアドレス」かについては、
一般的には以下の方法で確認することができます。

- システムベンダ・プロバイダとの契約内容を確認する

システムベンダ・プロバイダによっては、固定IPアドレスを有料オプションとしている場合があります。

契約書類中に、「固定IP」に関連する記載がないか、ご確認ください。

「固定IP」に関連する記載がない場合、ご使用のグローバルIPアドレスは「動的IP」の可能性が高いです。

詳細につきましては、院内の管理ご担当者様や、システムベンダ・プロバイダ様へ直接お問い合わせください。

- ルータやONUの設定画面を確認する

PPPoE設定や、WAN設定の画面にて、DHCPが有効になっているか、グローバルIPアドレスを装置上で直接設定しているかを
確認することができます。

詳細につきましては、システムベンダにご確認ください。

- 確認手順書に従って確認する

主要なメーカーの装置に関しては、確認手順書を準備しております。
ポータルシステムをご参照ください。

グローバルIPアドレスについては、システムベンダ様にご確認をお願いいたします。
※以下に記載の内容につきまして、医療機関様側で確認が必要になった場合にご参照ください。

関連スライド
:脆弱性診断関連の情報の
記入④

■ プレフィックス長とは

プレフィックス長とは、IPアドレスにおいて、「どこまでが同じネットワークか」という区切りを示す数字のことです。
IPアドレスの範囲(=サブネット)を表します。

プレフィックス長が「/32」であれば、特定の(ひとつの)IPアドレスのみを示します。

プレフィックス長が「/0」～「/31」であれば、複数のIPアドレスを含む範囲(ネットワーク)を示すこととなります。

※「/24」の場合、256個のIPアドレスの範囲を示します。

※「/0」の場合、すべてのIPアドレス(0.0.0.0～255.255.255.255)を含む、「全体」を示します。

■ 本事業において記載いただきたいプレフィックス長の範囲

本事業では、貴院にて使用されているIPアドレスを診断するため、IPアドレスを一意に特定する必要がございます。

プレフィックス長を「/24」に指定する等、複数のIPアドレスを含む範囲でご記載いただいた場合、

貴院で使用されているIPアドレスを特定することができず、脆弱性診断を実施することができません。

プレフィックス長は「/32」(※IPアドレスをひとつだけ指定する形式)をご指定ください。

補足⑥: 入力チェック

7. 追加説明資料

■ 入力チェック

入力いただいたIPアドレスについて、脆弱性診断が可能なグローバルIPアドレスか否かを確認する欄です。
「グローバルIPアドレス」欄にグローバルIPアドレスを記入いただくと、自動的に以下の5つの文言のうち1つが対象セル内に表示されます。
表示される文言を確認し、脆弱性診断が可能なグローバルIPアドレスであるかのチェックにご活用ください。
「入力チェック」欄には、新たに何かを記入いただく必要はございません。

関連スライド
:脆弱性診断関連の情報の
記入④

※「有効なIPアドレス」やプライベートIPアドレスについての詳細は、
[7. 追加説明資料【補足⑦: 脆弱性診断可能なIPアドレス】](#)をご参照ください。

No.	「入力チェック」欄に表示される文言	意味(詳細)
1	正しい値をご記入ください。	グローバルIPアドレスとして正しい形となっておりません。
2	プライベートIPアドレスが記載されていますので、再度ご確認をお願いいたします。	グローバルIPアドレスではなく、プライベートIPアドレスが記載されています。
3	脆弱性診断可能なグローバルIPアドレスであるかをご確認いただき、問題なければ「/32」とご指定ください。	プレフィックス長について、「/32」以外が指定されています。
4	脆弱性診断可能なグローバルIPアドレスでないようです。改めてIPアドレスをご確認ください。	No.1,2以外の理由で、脆弱性診断可能なグローバルIPアドレスではありません。
5	記載に問題ございません。	脆弱性診断実施可能なグローバルIPアドレスを記載いただいている。

補足⑦：脆弱性診断可能なIPアドレス

7. 追加説明資料

■ 「脆弱性診断可能なグローバルIPアドレス」について

「脆弱性診断可能なグローバルIPアドレス」とは、脆弱性診断にて診断が可能なグローバルIPアドレスのこと
を指します。

「脆弱性診断可能なグローバルIPアドレス」であるには、以下2点を満たしている必要がございます。

① リモートから接続可能であること

脆弱性診断では、該当するグローバルIPアドレスにリモートから接続いたします。

そのため、インターネット上の別の場所からそのグローバルIPアドレスに接続できる必要がございます。

これらから、プライベートIPアドレスはご指定いただくことができません。

※以下の範囲はすべてプライベートIPアドレスになり、脆弱性診断不可となります。

⇒10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 (※1)

また、通信形態「閉域網」についても、リモートからの接続が不可のため、脆弱性診断不可となります。

② 範囲指定されていない、一意に特定できるアドレスであること

脆弱性診断では、貴院にて使用されているIPアドレスを診断するため、IPアドレスを一意に特定する必
要がございます。

プレフィックス長を「/24」に指定する等、複数のIPアドレスを含む範囲でご記載いただいた場合、

貴院で使用されているIPアドレスを特定することができず、脆弱性診断を実施することができません。

プレフィックス長は「/32」(※IPアドレスをひとつだけ指定する形式)をご指定ください。

関連スライド
:脆弱性診断関連の情報の
記入④
:補足⑥:入力チェック

※1 プライベートIPアドレスの範囲

クラス	アドレス範囲
クラスA	10.0.0.0～10.255.255.255
クラスB	172.16.0.0～172.31.255.255
クラスC	192.168.0.0～192.168.255.255

補足⑧：脆弱性診断当日の流れ

7. 追加説明資料

- 最新版の「ヒアリングシート」にて、以下の2点に該当する回線については、本スライドの流れの通り、ご対応をお願いいたします。
①「脆弱性診断希望」欄について、「調査希望あり」を選択している。
②「固定IP/動的IP」欄について、「動的IP」を選択している。

関連スライド
：脆弱性診断関連の情報の
記入③,④

診断日前

■ 動的グローバルIPアドレスの記入は不要

診断日当日まで、「ヒアリングシート」上に
動的グローバルIPアドレスの記入は不要です。

診断当日

■ 動的グローバルIPアドレスの記入

ポータルシステム上に、動的グローバルIPアドレスをご登録いただきます。

①動的グローバルIPアドレスについて、脆弱性診断当日に確認したものを登録してください。

※ 動的グローバルIPアドレスについて、その性質上、IPアドレスが変動いたします。想定されていないグローバルIPアドレスへの
脆弱性診断の実施を防ぐため、当日のご確認にご協力ををお願いいたします。

②ご登録いただく時間について、脆弱性診断当日の午前0時から午前11時までとさせていただきます。

※当日午前0時から午前11時にのみ、ポータルシステム上への情報の登録が可能です。

※脆弱性診断当日の午前11時を過ぎてからご登録いただいた場合、診断不可となります。

診断実施

■ 脆弱性診断の実施

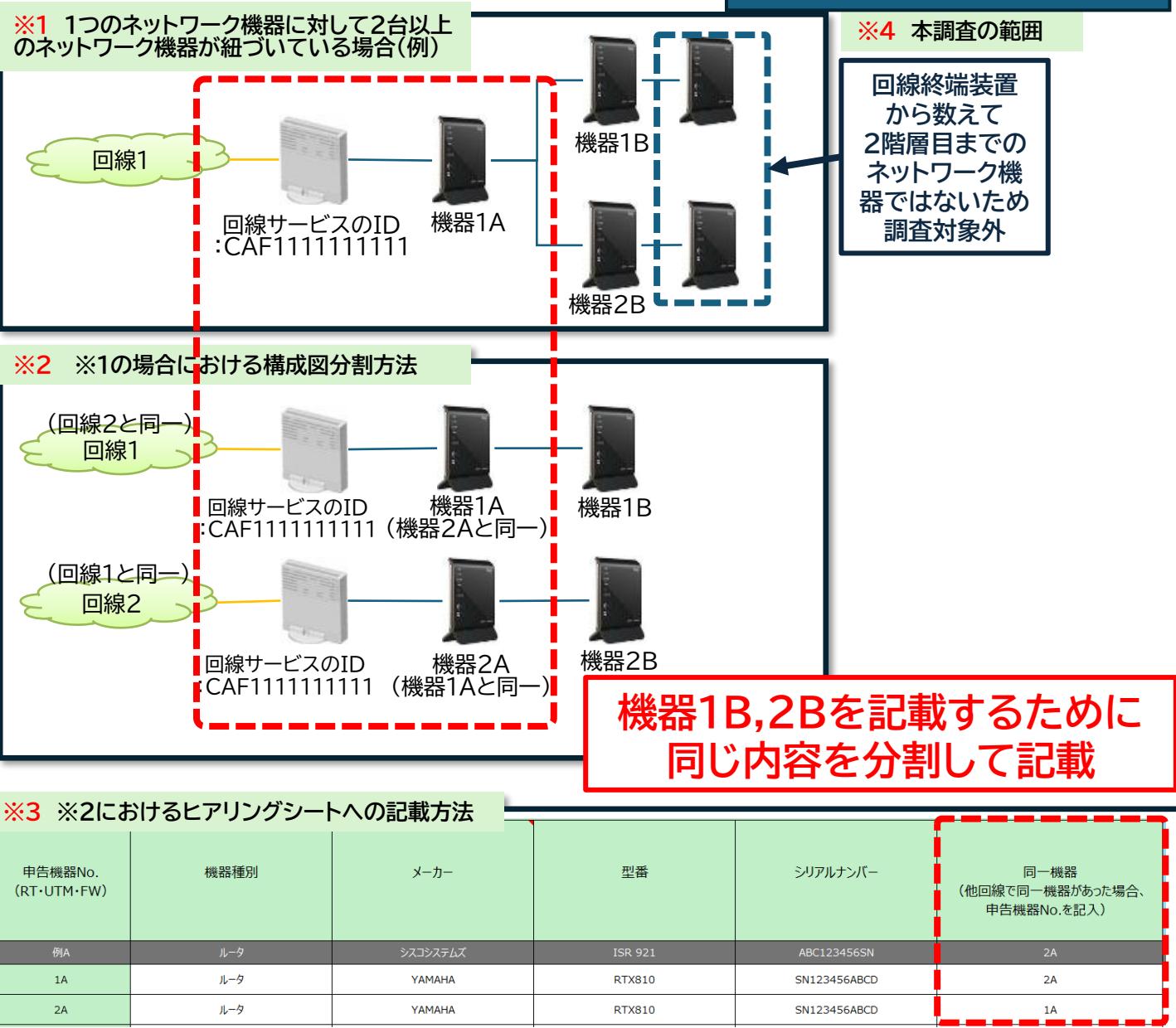
脆弱性診断当日に確認が取れた動的IPアドレスに対して、脆弱性診断を実施いたします。
(固定IPについては、事前に共有いただいたIPアドレスに対して診断を実施いたします。)

補足⑨:同一機器

関連スライド
:回線に紐づく機器情報の
記入②,⑥

- 同じ機器がほかの回線にも接続されている場合
(並列の機器がある場合)について
ヒアリングシートでは、同じ回線に紐づいている機器は最大2台までしかご記入いただけません。
(※回線終端装置に対して3階層以上ネットワーク機器(レイヤ3機器を指す/スイッチ等を除く)が紐づいていた場合、より回線終端装置に近い2階層分のみを、本事業における調査範囲としております(※4))

そのため、1つのネットワーク機器に対して2台以上のネットワーク機器が紐づいている場合(※1)、回線と、該当するネットワーク機器を分割してご記載ください(※2,※3)。



補足⑩：二要素認証

■ 二要素認証について

二要素認証とは、記憶・生体情報・物理媒体といった異なる認証手段のうち、2種類を組み合わせることにより、安全性を向上させることを目的とした認証方式のことです。

厚生労働省による「医療情報システムの安全管理に関するガイドライン」では、令和9年度時点で稼働していることが想定される医療情報システムを、新規導入または更新する場合、**二要素認証を採用するシステムの導入、またはこれに相当する対応を行う**ことを求めていました。

■ 二要素認証の採用例

- ・パスワード(記憶情報) + 指紋認証(生体情報)
- ・ICカード(物理媒体) + パスワード(記憶情報)
- ・ICカード(物理媒体) + 虹彩認証(生体情報)

関連スライド

:セキュリティ対策状況
パスワードポリシーの記入③

記憶情報

認証する人物が記憶している情報を使用する

- ・パスワード
- ・暗証番号(PIN)
- ・秘密の質問

生体情報

認証する人物の身体的特徴を使用する

- ・指紋認証
- ・顔認証
- ・網膜認証

物理媒体

認証する人物が所有しているものを使用する

- ・ICカード
- ・SMS認証
- ・ワンタイムパスワード