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

ご説明資料
ベンダ様向け調査説明資料

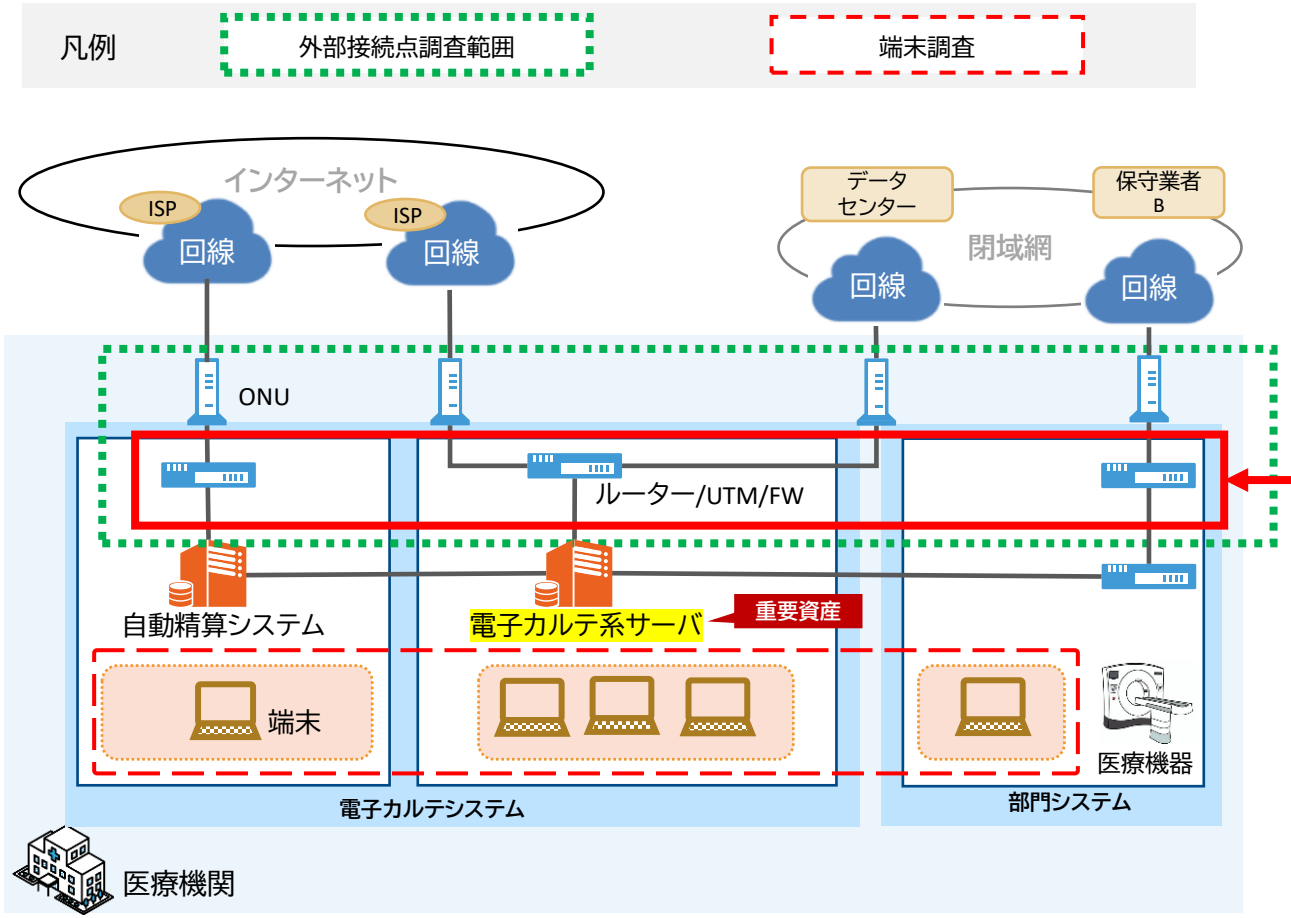
東日本電信電話株式会社　ビジネスイノベーション本部

目次

1. 調査内容＜現地調査＞

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）



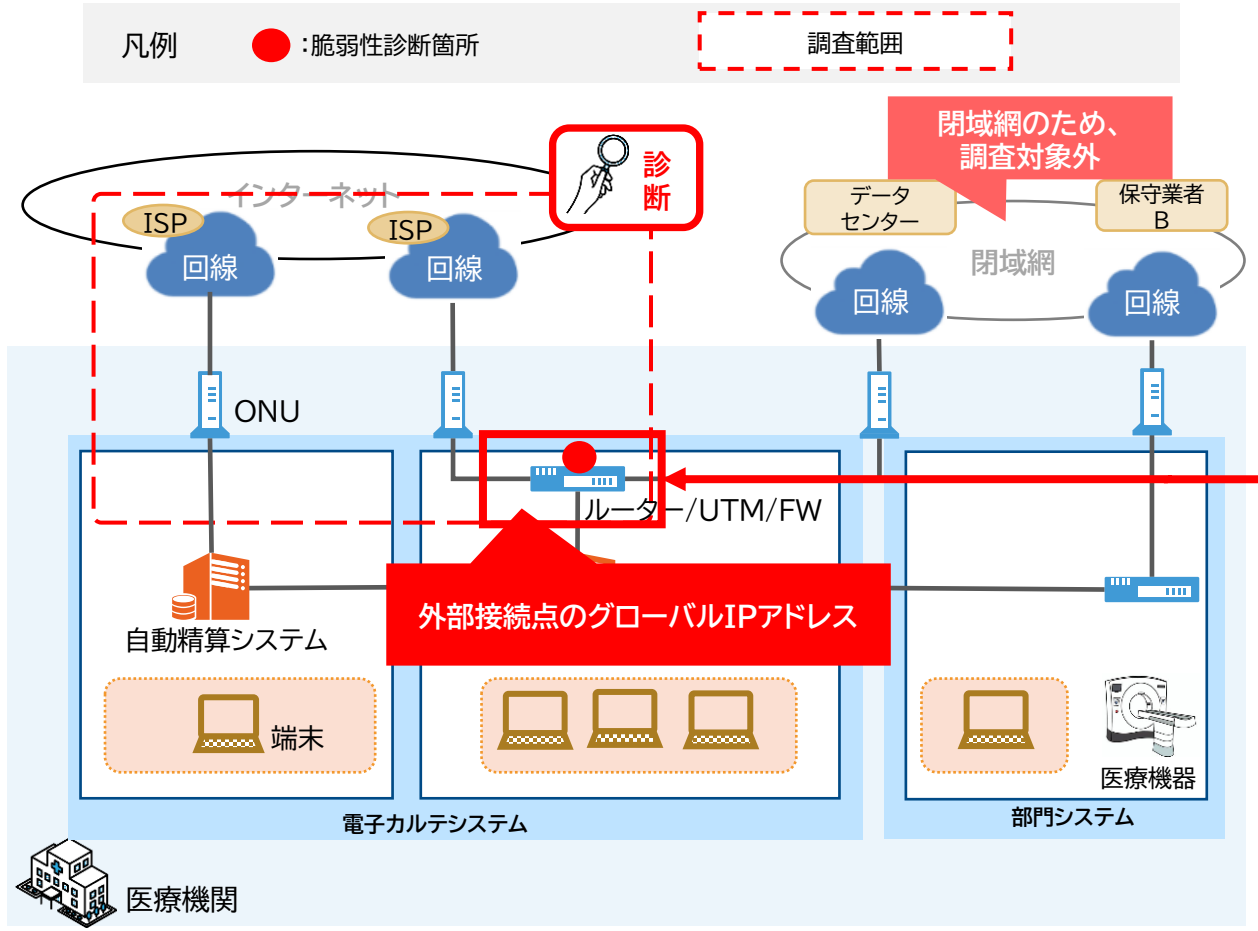
項目	内容
【調査目的】	外部接続点 • 病院の外部ネットワーク接続の俯瞰的把握、外部接続点の洗い出し 端末調査 • 端末のセキュリティ対策状況の調査
【調査内容】	外部接続点 • 外部接続点を中心とした物理構成の把握（回線を基準とした外部接続点周辺機器を対象） • 回線、ネットワーク機器の接続構成の目視確認 端末調査 • 電子カルテおよび主要な部門システム端末のOS、ウィルス対策ソフト等の設定確認（「【参考】現地調査について」参照）
【注意事項】	外部接続点 • 貴院で管理していない回線（例：ベンダー名義の保守用回線等）については、回線契約者にご協力いただく場合がございます。 • 調査対象機器のファームウェアのバージョンについては、事前にシステムベンダー等へ確認をお願いします。 端末調査 • 端末5台を上限として調査を実施します。 ・Windows10、Windows11の端末の選定をお願いします。Windows7も調査可能ですが、一部調査できない項目があるため、WIndows10/11を推奨します。（MacOSは対象外） • 対象端末は、電子カルテシステム接続する端末を1台以上選定してください。その他の端末は電子カルテシステムに接続されていれば、他システムで利用している端末で問題ありません。

ベンダ様ご協力依頼箇所

2. 調査内容＜脆弱性診断＞

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】	• 外部接続点のネットワーク機器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 -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。 • 脆弱性スキャン（TCP/UDP） -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。
【注意事項】	• 脆弱性診断の対象は、インターネット接続の外部接続点のネットワーク機器です。（サーバ等は対象外） • 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。 • 動的グローバルIPアドレスの場合、脆弱性診断実施日の午前11時までにグローバルIPアドレスをお知らせください。 • 動的グローバルIPアドレスの場合、IPアドレスの変動がなくても、診断日当日に連携をお願いします。 • 早期に対応が必要な脆弱性が見つかった場合、調査結果報告書とは別に、簡易報告を実施します。

ベンダ様
ご協力依頼箇所

- 脆弱性診断実施条件の詳細は次頁ご確認ください。

2. 脆弱性診断について

- **脆弱性診断の流れは以下の通りです。**

1 ヒアリング

- ✓ インターネットアクセスのある回線か、インターネットVPN用の回線か（閉域網に接続された回線は対象外）
- ✓ グローバルIPアドレスを持つ機器の確認
- ✓ グローバルIPアドレスは固定IPか、動的IPか
- ✓ 対象回線が接続されるネットワーク/システムが、電子カルテシステムの所属するネットワークと接続があるか
- ✓ 脆弱性診断の実施候補日時（現地調査日の翌営業日から5営業日以内を想定）
- ✓ 脆弱性診断実施に伴う静観対応（監視）の対応依頼

2 診断

診断開始日時の連絡、および診断完了後、ご報告いたします。

- ✓ 動的グローバルIPアドレスの場合、診断実施当日にIPアドレスの連携をお願いします
- ✓ 脆弱性診断の実施（所要時間：1日当たり2～24時間）
  - ※ 回線数および診断状況により日数は変動する可能性があります
  - ※ リモートで診断となるため、当日の立ち合いは不要です

■脆弱性診断による業務影響について
・脆弱性診断による業務影響は発生しない想定です。

3 分析

- ✓ 診断の分析、報告書とりまとめ（NTT東日本）

4 報告

結果を医療機関様にお知らせします。（調査実施後2ヶ月（目安））

- ✓ 診断結果の報告書提出（NTT東日本）
  - ※ ポートスキャン、脆弱性スキャンの結果を報告

診断結果			
	緊急（9.0～10.0）	：	0件
	重要（7.0～8.9）	：	0件
	警告（4.0～6.9）	：	0件
	注意（0.1～3.9）	：	0件
	対処要	：	0件
	対処推奨	：	1件

2. 脆弱性診断について

- 脆弱性診断における実施条件と、必要情報について、下記表をご参照ください。

通信形態	固定IP/動的IP	グローバルIPアドレス		診断実施	備考
		ヒアリングシート記入	脆弱性診断当日連携		
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	-	-	-	×	

3. 対象装置の情報提供依頼

- 本事業の「①外部ネットワーク接続の俯瞰的把握、安全性を検証」の一環として、医療機関の電子カルテシステムに接続されている回線・機器の洗い出しを実施します。
- 洗い出した回線に紐づく機器（ルータ/ファイアウォール/UTM）の脆弱性情報の確認を実施します。
  そのため、機器のファームウェアバージョンをヒアリングシートに記入いただきます。
- 洗い出した回線に紐づく機器（ルータ/ファイアウォール/UTM）がグローバルIPアドレスを有している場合、リモートからの脆弱性診断を実施します（希望ありの場合）。
  そのため、グローバルIPアドレスをヒアリングシートに記入いただきます。
- 医療機関管理下の回線・機器以外にも、ベンダ様にて管理している回線や機器も調査対象としているため、医療機関への情報提供の協力をお願いいたします。

必要情報	説明
ファームウェアバージョン	• 対象装置のファームウェアバージョンに既知の脆弱性がないか確認します。 • そのため、稼働中のファームウェアバージョンの情報をご教示ください。
グローバルIPアドレス	• 対象装置が有するグローバルIPアドレスに対して、脆弱性診断を実施します。 • そのため、外部接続点のWANポートに紐づくグローバルIPアドレスの情報をご教示ください。

3. 対象装置の情報提供依頼

- ベンダ様へのご依頼事項となりますので、下記いずれかの対応、ご協力をお願いいたします。

依頼事項	詳細
ベンダ様にて対象装置（ルータ/ファイアウォール/UTM）の情報取得	・回線に紐づく装置のファームウェアバージョン情報、およびグローバルIPアドレスを実機で確認し確認結果を医療機関様にお伝えください。 ・グローバルIPアドレスについては、固定IPか動的IPか、プロバイダ契約情報を確認いただき、医療機関様にお伝えください。
医療機関様への情報取得方法の展開	・ベンダ様による対応が困難な場合、医療機関ご担当者様にて該当の情報を確認頂くことを検討しています。 ・つきまして、医療機関様への情報取得手順の展開をお願いします。 - 装置へのログイン方法 - ファームウェアバージョンの確認方法 - ルーティング情報（グローバルIPアドレス）の確認方法 ・グローバルIPアドレスについては、固定IPか動的IPか、プロバイダ契約情報を確認いただき、医療機関様にお伝えください。

3. 対象装置の情報提供依頼

- ベンダ様へのご依頼事項となりますので、ご協力の程、よろしくお願いいたします。

依頼事項	詳細
対象回線・機器の妥当性確認	回線種別やグローバルIPアドレスをもつ機器の妥当性の確認をお願いいたします。 - インターネットアクセスのある回線、またはインターネットVPN用回線であること - 閉域網(IP-VPNなど)の回線は対象外
グローバルIPアドレスの妥当性確認	正しく脆弱性診断が実施できるよう、グローバルIPアドレスの妥当性の確認をお願いいたします。 - グローバルIPアドレスと対象機器が一致していること - グローバルIPアドレスが固定IPか動的IPか
診断実施日時の妥当性確認	業務影響なく脆弱性診断を実施するため、診断実施日時の妥当性の確認をお願いいたします。 - 避けるべき時間帯、予定されているイベント(法定停電など)を回避した日時になっているか
診断実施日のグローバルIPアドレス確認	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 -医療機関担当者へグローバルIPアドレスの情報取得方法の展開が可能か - ベンダ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。 - 脆弱性診断の送信元IPアドレスは別途周知します。