はじめに

本資料は、YouTube概要欄からダウンロード可能です
動画と併せてご覧ください

厚生労働省「R7年度_医療機関におけるサイバーセキュリティ確保事業」

【医療機関様向け】外部ネットワーク接続点調査報告書補足説明資料(第1.0版)

2025年9月12日　NTT東日本株式会社

本資料・動画の活用について

- 本資料・動画は、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」における「外部ネットワーク接続の俯瞰的把握、安全性の検証・調査」の結果をとりまとめた**「外部ネットワーク接続点調査報告書」（以下、調査報告書）の解説となります。**
（外部ネットワーク接続点調査報告書本紙・別紙の関連性、各ページの読み方を主に補足しています）

- 調査報告書は、医療機関の現状把握と改善検討のための正確な基礎資料となります。これを元にベンダと相談し、適切なセキュリティ対策を進めてください。

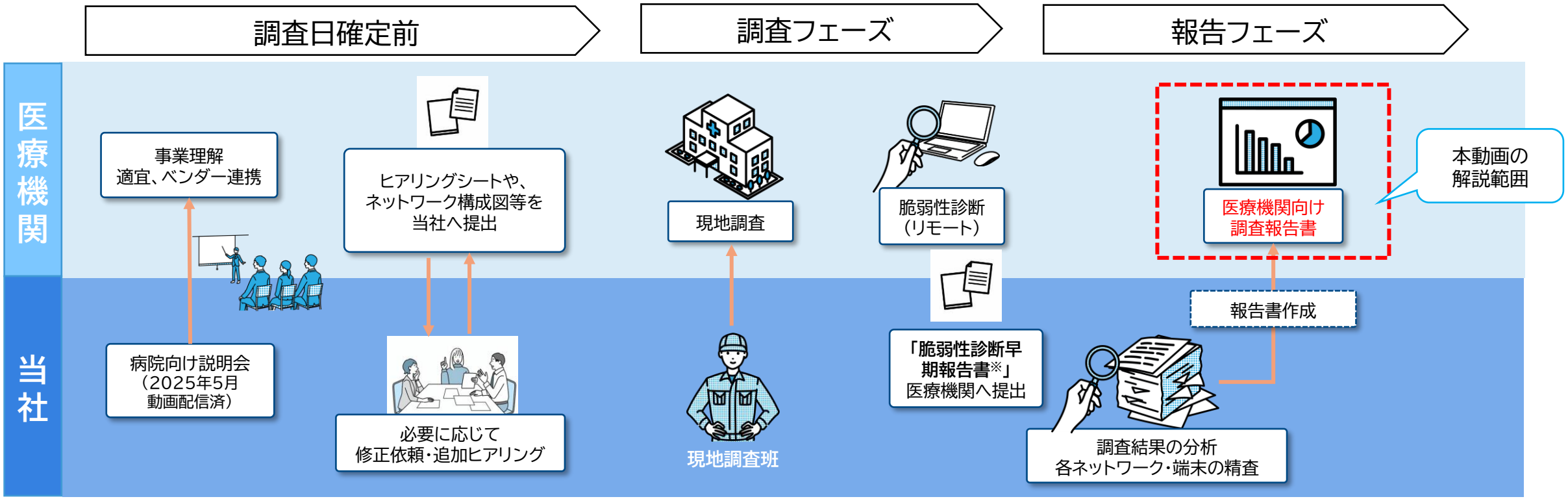
- 外部ネットワーク接続点調査報告書は、現地調査および脆弱性診断の実施後から**2か月後を目安に、セキュリティ確保事業ポータル（Kintone）（以下、ポータルシステム）にアップロードしています。** *取得方法はP.3をご参照下さい。

- 事前に以下をお手元にご用意の上、ご視聴下さい。
  ・「外部ネットワーク接続点調査報告書」（以下、**調査報告書**）
  ・「ヒアリングシート」
  ※最終確定版はポータルシステムの「03_ヒアリングシート提出アプリ」下部の情報をご確認ください

- 本事業概要、実施内容等の詳細については、以下の病院説明会動画および医療機関向け説明会資料をご参照下さい。
  URL再掲：https://www.youtube.com/watch?v=4wHEl8DfsTg
  YouTube 厚生労働省チャネル上に限定公開

これまでの調査経緯と調査報告書の位置づけについて

- 医療機関にて収集いただいた回線・ネットワーク機器等の情報を基に、現地調査および脆弱性診断を実施しています。
- ご提出いただいたヒアリングシートと合わせてご確認ください。



※「脆弱性診断早期報告書」は、脆弱性診断によって緊急性の高いセキュリティリスクが発見された場合にのみ、作成・送付します。

参考　脆弱性診断早期報告書、調査報告書の取得方法（抜粋）

- 脆弱性診断早期報告書、調査報告書は、<u>ポータルシステムの「04 ファイル共有アプリ」より取得をお願いします。</u>
  ※セキュリティ確保事業ポータルの利用ができない医療機関に対しては、事務局よりメールにて送付しています。

＜メール通知からアクセスする方法＞※その他のアクセス方法や詳細はポータルシステム内のマニュアルをご確認下さい。

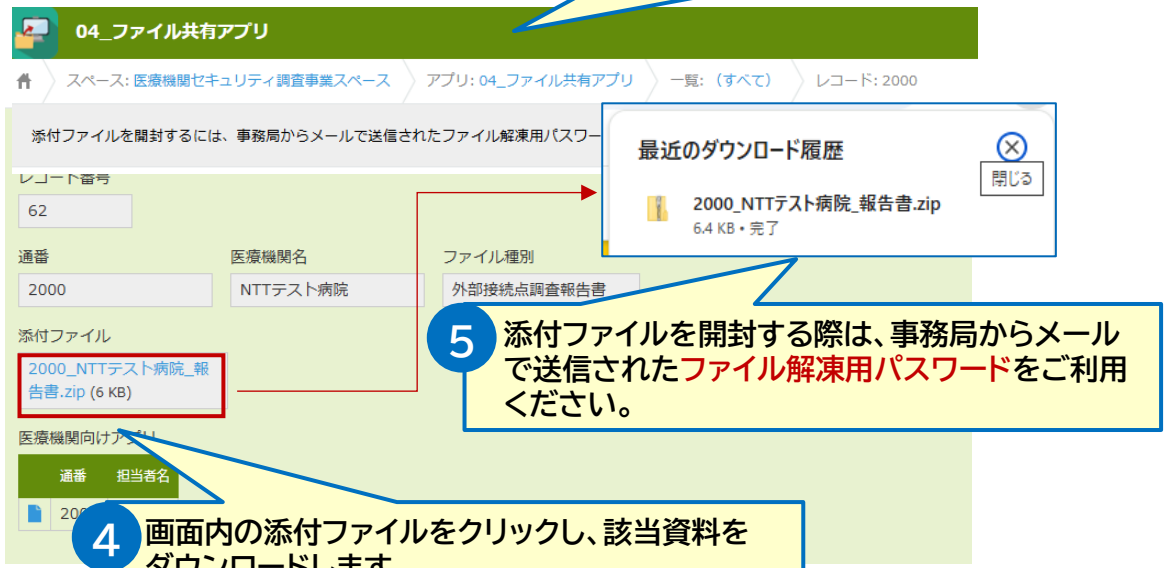
Step 1	資料がアップロードされると、kintone（no-reply@cybozu.com）より病院担当者様宛に通知メールが届く

Step 2	ポータルシステム（Kintone）内の「04_ファイル共有アプリ」より資料を取得

1 メール文中の「レコードを表示」をクリックします

2 ログイン画面に遷移するので、ログイン操作を行います

3 ログイン後、自動的に下記の画面に遷移します



4 画面内の添付ファイルをクリックし、該当資料をダウンロードします

5 添付ファイルを開封する際は、事務局からメールで送信されたファイル解凍用パスワードをご利用ください。

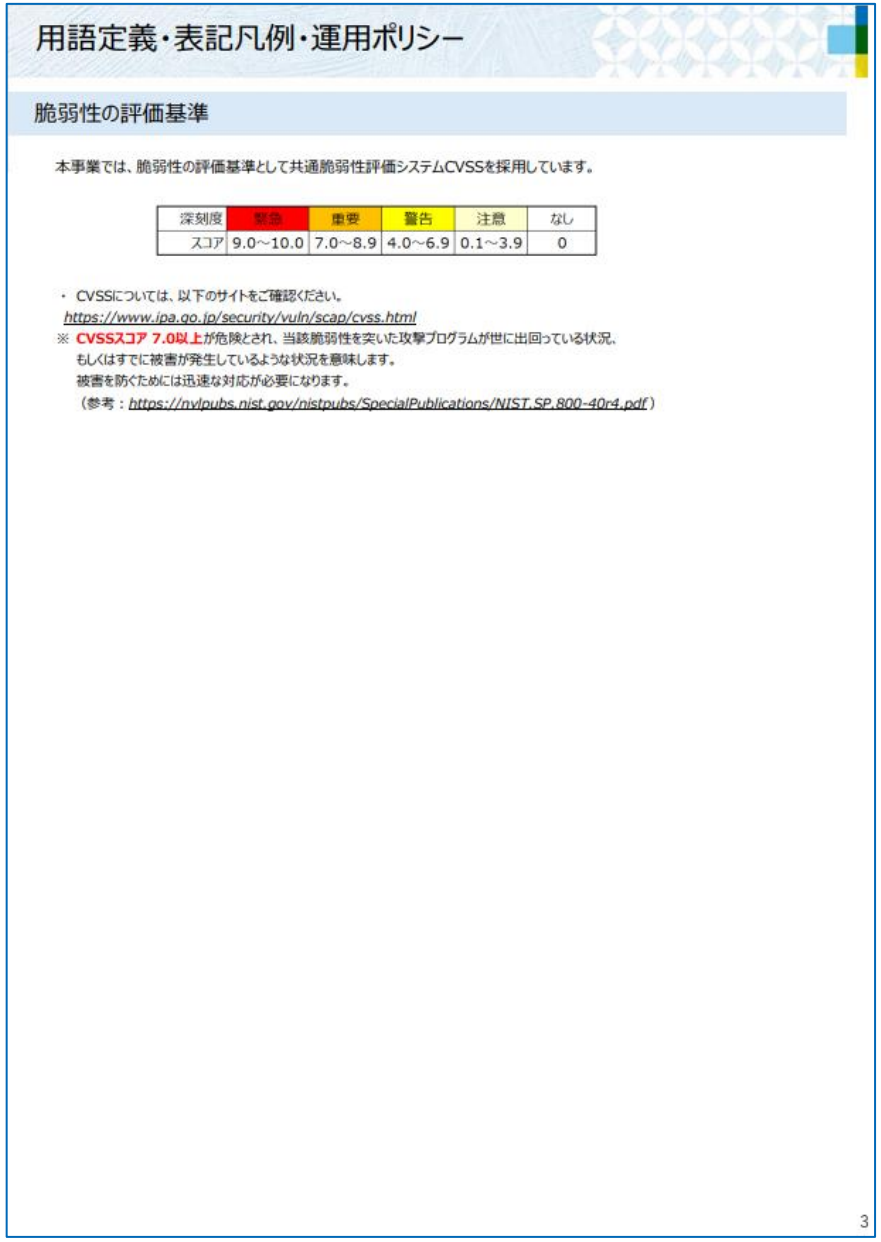
- 「外部ネットワーク接続点調査報告書」は調査実施後、2か月後を目安にアップロードされます

目次

「外部ネットワーク接続点調査報告書」の補足説明

「用語定義・表記凡例・運用ポリシー」に関して

「用語定義・表記凡例・運用ポリシー（脆弱性の評価基準）」に関して


用語定義・表記凡例・運用ポリシー

脆弱性の評価基準

本事業では、脆弱性の評価基準として共通脆弱性評価システムCVSSを採用しています。

深刻度	緊急	重要	警告	注意	なし
スコア	9.0～10.0	7.0～8.9	4.0～6.9	0.1～3.9	0

・ CVSSについては、以下のサイトをご確認ください。
https://www.ipa.go.jp/security/vuln/scap/cvss.html
※ CVSSスコア 7.0以上が危険とされ、当該脆弱性を突いた攻撃プログラムが世に出回っている状況、もしくはすでに被害が発生しているような状況を意味します。
被害を防ぐためには迅速な対応が必要になります。
（参考：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf）

3

補足ポイント

■脆弱性の評価基準について記載しています。
本事業では、国際的な指標である「共通脆弱性評価システム（CVSS）」を採用しています。値の算出方法は、下記サイトの「3.値の算出方法」に記載があります。
共通脆弱性評価システムCVSS v3概説 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
緊急・重要（CVSS7.0以上）は、当該脆弱性を突いた攻撃プログラムが世に出回っている状況、もしくはすでに被害が発生しているような状況を意味しているため、被害を防ぐためには早急な対応が必要です。


3. 値の算出方法

CVSSでは、(1)脆弱性の技術的な特性を評価する基準（基本評価基準：Base Metrics）、(2)ある時点における脆弱性を取り巻く状況を評価する基準（現状評価基準：Temporal Metrics）、(3)利用者環境における問題の大きさを評価する基準（環境評価基準：Environmental Metrics）を順番に評価していくことで、脆弱性の深刻度を0（低）～10.0（高）の数値で表します。

(1)深刻度レベル分け
CVSS v3では、深刻度レベル分けを次のように設定しています。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

出典：IPA 独立行政法人 情報処理推進機構　https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

※各章でのCVSS値の対象バージョンは以下の通りです。
・**5. 外部ネットワーク接続機器調査**
可能な限り新しいバージョンでCVSS値を報告します。
上記のいずれかのバージョンでのCVSS値が確認できなかった場合は、「-」（ハイフン）と記載されます。
※優先バージョンはv4.0 → v3.1 → v3.0 → v2.0 → v1.0
・**4. 脆弱性診断**
一律でv3.0を採用します。

「1.調査結果　総括」に関して

「1-1. 調査結果 総括表」に関して

1-1. 調査結果 総括表

調査実施日

調査日	現地調査開始日	2025年7月28日
	脆弱性診断開始日	2025年8月4日
	脆弱性情報確認	2025年8月末時点での脆弱性情報を基にしています。

調査結果　総括表

・外部ネットワーク接続の俯瞰的把握

調査項目		件数	参照先章番号
外部ネットワーク接続点および その配下のネットワーク機器の洗い出し・把握	事前申告いただいた回線		2章 3章
	事前申告情報と照合できた回線	3件	
	現地調査で照合できなかったネットワーク機器	2件	
	現地調査で照合できなかった回線	2件	
	事前申告されていなかった回線		
	現地調査で新規に検出した回線	1件	
	新規検出回線配下で新規検出された機器	1件	

※「事前申告情報と照合できた回線」と「事前申告情報と照合できなかった回線」の合計値が、ヒアリングシートにて事前申告いただいた回線の総数となります。
※「新規検出回線配下で新規検出された機器」について、現地で新規に検出した回線に紐づくネットワーク機器のみ件数として計上しています。

・セキュリティ対策等の調査

調査項目		件数	参照先章番号
脆弱性診断	脆弱性診断対象のグローバルIPアドレス		4章
	調査対象のグローバルIPアドレス数	1件	
	脆弱性情報検出ありのグローバルIPアドレス数	1件	
外部ネットワーク接続機器 脆弱性調査	調査対象のネットワーク機器		5章
	脆弱性情報検出ありのネットワーク機器数	5件	
	ファームウェアが最新ではない	2件	
端末セキュリティ対策	調査端末		6章
	OSサポートなし	0件	
	セキュリティ対策ソフトなし	0件	
	USB使用制限なし	1件	
パスワードポリシー	外部ネットワーク接続機器調査（有効回答分）		5章
	ポリシーに適合していない	3件	
	アカウントの使い回しをしている	1件	
	調査端末（有効回答分）		6章
	ポリシーに適合していない	1件	
	アカウントの使い回しをしている	2件	

※ 貴院から希望のなかった調査項目や、調査ができなかった項目について、「-」にて示しています。

7

補足ポイント

❶現地で照合できなかったネットワーク機器
下記の機器が対象になります。
・申告された機器のうち、現地で確認できなかった機器
・申告された回線の配下で、現地で新たに確認された機器

❷現地調査で照合できなかった回線
3. 外部ネットワーク接続点の洗い出し・把握の「差分」が「あり」または「-（ハイフン）」になっている回線が対象となります。

3. 外部ネットワーク接続点の洗い出し・把握

申告回線No.	事前申告情報				現地調査情報		調査結果
	回線サービス名	回線サービスのID	用途・システム名	通信形態	差分	回線サービスのID	
1	フレッツ光	CAF1111111111	電子カルテシステム	インターネットVPN	なし	CAF1111111111	・ご申告いただいた回線サービスのIDが、現地調査でも確認できました。
2	DOCOMO	不明	医療機器	インターネット	－	不明	・現地にてご案内いただいた情報をもとに回線を記載しております。現地調査において、回線サービスのIDの確認ができませんでした。改めて対象回線の情報を確認し、適切な管理をお願いします。

❸現地で新規に検出した回線/新規検出回線配下で新規検出された機器
現地調査時に「その他回線調査」をご希望された場合、申告いただいた回線の他に回線が存在しないかを調査します。
新規に回線及び配下の機器が検出された場合、**3. 外部ネットワーク接続点の洗い出し・把握**の最終ページに記載されます。貴院で管理されている回線かどうかご確認をお願いいたします。

「1-2. 調査結果 総括文言」に関して

1-2. 調査結果 総括文言

調査結果　総括文言 1/2

本事業に関する調査結果の総括を、以下にご報告いたします。

総括

1 外部ネットワーク接続の俯瞰的把握

「外部ネットワーク接続の俯瞰的把握」における外部ネットワーク接続点としては、事前に申告いただいた回線のうち、回線終端装置の確認ができなかった回線がありました。また、事前に申告いただいた回線以外の回線終端装置が現地調査で確認されました。本調査対象外の回線（電子カルテシステムへの接続がない回線）の可能性もありますが、あらためて利用用途等の確認をお願いします。

「外部ネットワーク接続の俯瞰的把握」におけるネットワーク機器としては、事前に申告いただいたネットワーク機器のうち、確認できなかった機器がありました。あらためて設置場所の確認をお願いします。また、事前に申告いただいていないネットワーク機器も現地調査で確認しています。

外部接続回線、およびその周辺の接続機器の管理は、セキュリティ対策上非常に重要であるため、引き続き適切な管理をお願いします。調査結果の詳細については、「2. 現地調査結果一覧」、および「3. 外部ネットワーク接続点の洗い出し・把握」をご確認ください。

脆弱性診断

「セキュリティ対策等の調査」における脆弱性診断では、調査対象IPアドレスに対してポートスキャン/インターネットからアクセス可能なポートを確認したところ、確認したすべてのIPアドレスにおいて脆弱性が検出されました。調査結果の詳細を確認いただき、適切な対応をお願いします。

調査結果の詳細については、「4. 脆弱性診断」をご確認ください。

外部ネットワーク接続機器 脆弱性調査

「セキュリティ対策等の調査」における外部ネットワーク接続機器の脆弱性調査では、ファームウェアバージョンで脆弱性情報の調査をしたネットワーク機器のうち、脆弱性が検出された機器がありました。一方で、現時点での最新ファームウェアを適用していない機器を確認しております。ネットワーク管理者(ベンダー等)と協議し、アップデート等適切な対応をご検討ください。ネットワーク機器の脆弱性を悪用したサイバー攻撃も増加しているため、引き続き定期的なファームウェアのアップデート・脆弱性情報の確認をお願いします。

調査結果の詳細については、「5. 外部ネットワーク接続機器調査」をご確認ください。

8

補足ポイント

❶総括文言の各項目について

前ページ**1-1. 調査結果 総括表**の項目(赤枠)に沿って調査結果を記載しております。
管理状況をご確認のうえ、必要に応じてネットワーク管理者及び各ベンダにご確認ください。

1-1. 調査結果 総括表

調査項目		件数	参照先章番号
外部ネットワーク接続点および その配下のネットワーク機器の洗い出し・把握	事前申告いただいた回線		2章 3章
	事前申告情報と照合できた回線	3件	
	現地調査で照合できたネットワーク機器	5件	
	現地調査で照合できなかったネットワーク機器	2件	
	現地調査で照合できなかった回線	2件	
	事前申告されていなかった回線		
	現地調査で新規に検出した回線	1件	
	新規検出回線配下で新規検出された機器	1件	

※「事前申告情報と照合できた回線」と「事前申告情報と照合できなかった回線」の合計値が、ヒアリングシートにて事前申告いただいた回線の総数となります。
※「新規検出回線配下で新規検出された機器」について、現地で新規に検出した回線に紐づくネットワーク機器のみ件数として計上しています。

・セキュリティ対策等の調査

調査項目		件数	参照先章番号
脆弱性診断	脆弱性診断対象のグローバルIPアドレス		4章
	調査対象のグローバルIPアドレス数	1件	
	脆弱性情報検出ありのグローバルIPアドレス数	1件	
外部ネットワーク接続機器 脆弱性調査	調査対象のネットワーク機器		5章
	脆弱性情報検出ありのネットワーク機器数	5件	
	ファームウェアが最新ではない	2件	
端末セキュリティ対策	調査端末		6章
	OSサポートなし	0件	
	セキュリティ対策ソフトなし	0件	
	USB使用制限なし	1件	
パスワードポリシー	外部ネットワーク接続機器調査（有効回答分）		5章
	ポリシーに適合していない	3件	
	アカウントの使い回しをしている	1件	
	調査端末（有効回答分）		6章
	ポリシーに適合していない	1件	
	アカウントの使い回しをしている	2件	

※ 貴院から希望のなかった調査項目や、調査ができなかった項目について、「-」にて示しています。

「2.現地調査結果一覧」に関して

「2-2. 現地調査結果一覧（機器一覧）」に関して

2-2. 現地調査結果一覧（機器一覧）

機器一覧

貴院の外部ネットワーク接続点を調査した結果を記載しています。

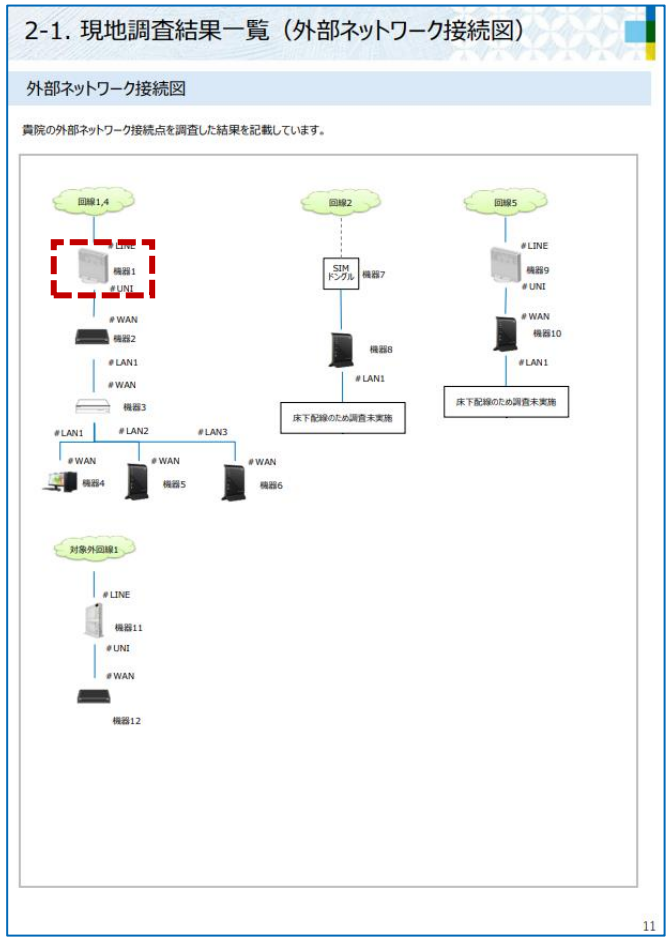
調査機器No.	機器情報				機器の紐づく回線情報	
	機器種別	メーカー名	型番	シリアルナンバー	調査回線No.	回線サービスのID
1	回線終端装置	NTT東日本	GE-PON-ONU	XXXXXXXXX1	1,4	CAF1111111111
2	ファイアウォール/UTM	フォーティネット(Fortinet)	FortiGate200F	FG200F111111111111	1,4	-
3	スイッチ	シスコシステムズ(Cisco)	Catalyst9300	調査未実施	1,4	-
4	端末(PC、サーバ)	ヒューレット・パッカード・エンタープライズ	HP EliteBook 630 G10	XXXX3	1,4	-
5	ルータ	ヤマハ(YAMAHA)	RTX1300	調査未実施	1	-
6	ルータ	ヤマハ(YAMAHA)	RTX1210	XXXXXXXXX30	4	-
7	SIMドングル	アイ・オー・データ	UD-USC1	XXXXXXXXXX22	2	調査未実施
8	ルータ	ヤマハ(YAMAHA)	RTX1220	XXXXXXXXX28	2	-
9	回線終端装置	SONY	FG4023B	調査未実施	5	xXXXXXXXX1
10	ルータ	日本電気(NEC)	UNIVERGE IX2107	XXX33	5	-
11	ONU内臓ルータ	NTT東日本	PR-500MI	調査未実施	対象外回線1	CAF5555555555
12	ファイアウォール/UTM	フォーティネット(Fortinet)	Foritigate400F	調査未実施	対象外回線1	-
13						
14						
15						
16						
17						
18						
19						
20						

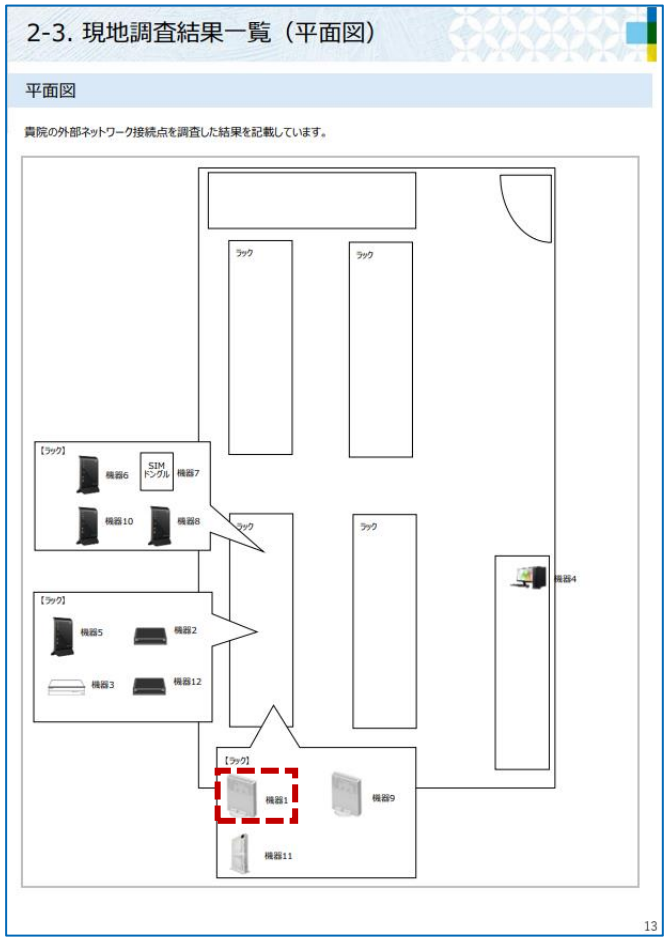
12

補足ポイント

❶調査機器No.

調査機器No.を基準に、外部ネットワーク接続図と平面図と照合し、貴院の把握状況と差分がないかご確認ください。「調査機器No.1」は「機器1」を指しています。





「3. 外部ネットワーク接続点の洗い出し・把握 」に関して

「3. 外部ネットワーク接続点の洗い出し・把握」に関して

3. 外部ネットワーク接続点の洗い出し・把握

外部ネットワーク接続点一覧 1/2

貴院の外部ネットワーク接続点を調査した結果を記載しています。

申告回線No.	事前申告情報				現地調査情報		調査結果
	回線サービス名	回線サービスのID	用途・システム名	通信形態	差分	回線サービスのID	
1	フレッツ光	CAF1111111111	電子カルテシステム	インターネットVPN	なし	CAF1111111111	・ご申告いただいた回線サービスのIDが、現地調査でも確認できました。
2	DOCOMO	不明	医療機器	インターネット	－	不明	・現地にてご案内いただいた情報をもとに回線を記載しております。現地調査において、回線サービスのIDの確認ができませんでした。改めて対象回線の情報を確認し、適切な管理をお願いします。
3	フレッツ光	CAF3333333333	医療事務・会計システム	閉域網	-	-	・ご申告いただいた回線サービスのIDを、現地調査では確認ができませんでした。改めて対象回線の情報を確認し、適切な管理をお願いします。
4	フレッツ光	CAF1111111111	電子カルテシステム	インターネットVPN	なし	CAF1111111111	・ご申告いただいた回線サービスのIDが、現地調査でも確認できました。
5	au光	xXXXXXXXX1	部門システム	インターネット	なし	xXXXXXXXX1	・ご申告いただいた回線サービスのIDが、現地調査でも確認できました。

15

補足ポイント

❶事前申告情報

ヒアリングシートで申告いただいた内容を転記しています。

ヒアリングシート　回線情報シート

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
01	フレッツ光	CAF1111111111	3F　サーバー室	電子カルテシステム
02	DOCOMO		3F　サーバー室	医療機器
03	フレッツ光	CAF3333333333	3F　サーバー室	医療事務・会計システム
04	フレッツ光	CAF1111111112	3F　サーバー室	電子カルテシステム
05	au光	xXXXXXXXX1	3F　サーバー室	部門システム

❷差分

「ヒアリングシートに記載いただいた回線情報」と「現地調査で確認できた回線」とで整合性が取れているかを示しています。内容をご確認の上、差分がある場合には、必要に応じてネットワーク管理者及び各ベンダにご確認ください。

※医療機関のネットワークへの影響を考慮し、ケーブルがまとめられている場合や床下配線等で調査が困難な状況である場合、現地で確認作業を実施していません。

「3. 外部ネットワーク接続点の洗い出し・把握」に関して

補足ポイント

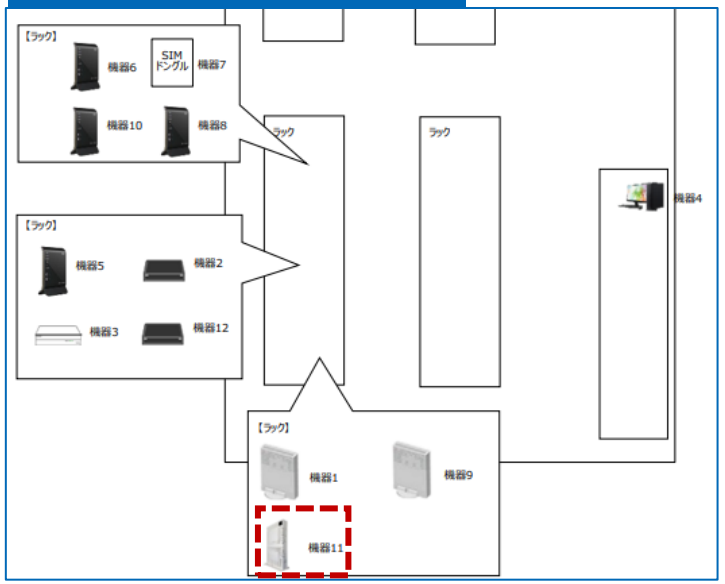
■「その他回線調査」を実施し、ヒアリングシートに記載がなかった回線終端装置及びその配下のネットワーク機器が現地で新たに確認された場合、左図のように対象外回線として報告されます。医療機関で把握されていない回線の場合は、必要に応じてネットワーク管理者及び各ベンダにご確認ください。
※対象外回線として報告されたものについて、電子カルテシステムの所属するネットワークとの接続がない回線である場合がありますので、ご了承ください。

❶調査機器No.
2-1. 現地調査結果一覧(機器一覧)、2-3. 現地調査結果一覧(平面図)を参照し、該当の調査機器No.をご確認ください。

2-1. 現地調査結果一覧(機器一覧)

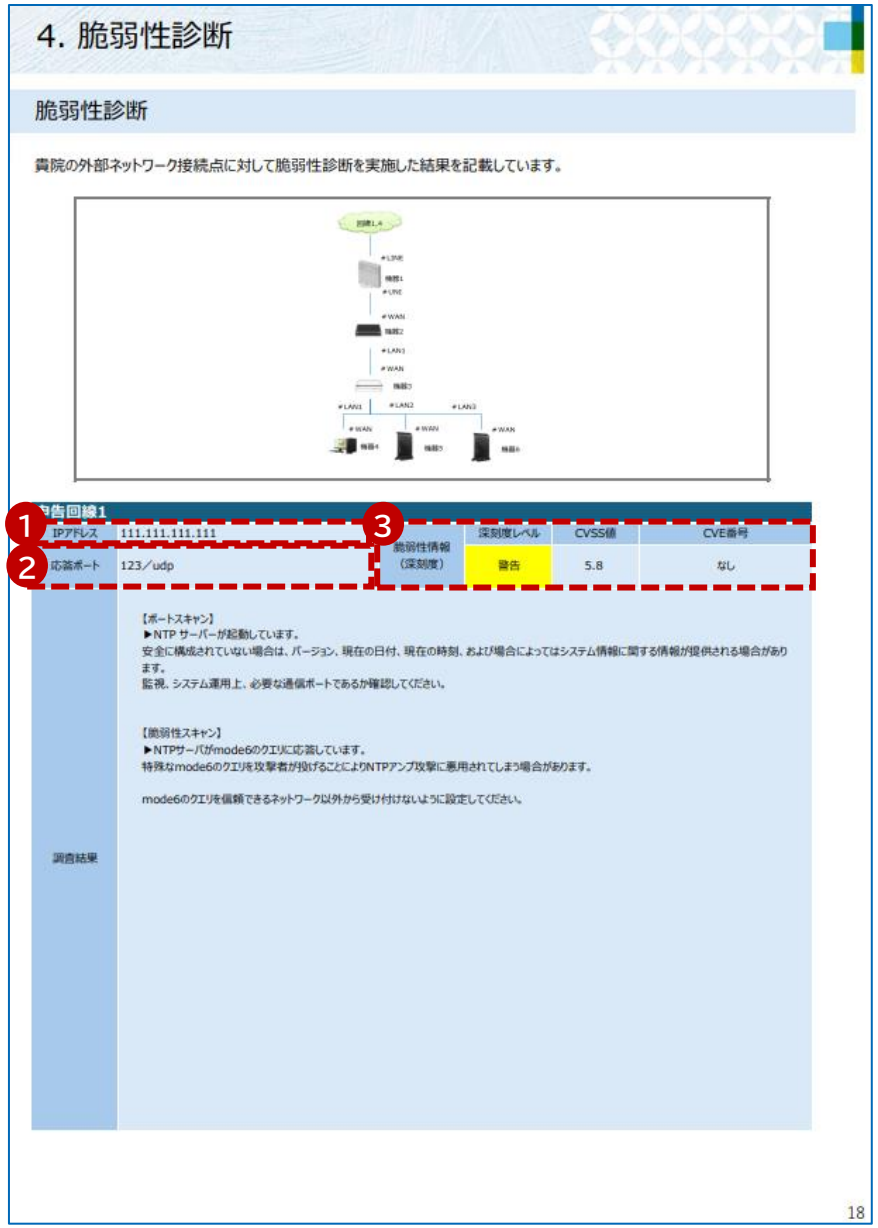
調査機器No.	機器情報			
	機器種別	メーカー名	型番	シリアルナンバー
1	回線終端装置	NTT東日本	GE-PON-ONU	XXXXXXXXX1
2	ファイアウォール/UTM	フォーティネット(Fortinet)	FortiGate200F	FG200F111111111111
3	スイッチ	シスコシステムズ(Cisco)	Catalyst9300	調査未実施
4	端末(PC、サーバ)	ヒューレット・パッカード・エンタープライズ	HP EliteBook 630 G10	XXXX3
5	ルータ	ヤマハ(YAMAHA)	RTX1300	調査未実施
6	ルータ	ヤマハ(YAMAHA)	RTX1210	XXXXXXXXX30
7	SIMドングル	アイ・オー・データ	UD-USC1	XXXXXXXXXX22
8	ルータ	ヤマハ(YAMAHA)	RTX1220	XXXXXXXXX28
9	回線終端装置	SONY	FG4023B	調査未実施
10	ルータ	日本電気(NEC)	UNIVERGE IX2107	XXX33
11	ONU内臓ルータ	NTT東日本	PR-500MI	調査未実施
12	ファイアウォール/UTM	フォーティネット(Fortinet)	Foritigate400F	調査未実施

2-3. 現地調査結果一覧(平面図)



「4.脆弱性診断」に関して

「4. 脆弱性診断」に関して



補足ポイント

❶IPアドレス

ヒアリングシートにて診断希望ありと申告いただいたグローバルIPアドレスに対し、脆弱性診断を実施しています。

ヒアリングシート　回線情報シート

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VPN	固定IP	111.111.111.111	/32		機器A

❷応答ポート

ポートスキャンを実施し、外部からアクセス可能なポートが検出された場合、ポート番号が記載されます。

❸脆弱性情報（深刻度）

❷で検出されたポートがあった場合、そのポートに対して脆弱性スキャンを実施します。
巻頭「用語定義・表記凡例・運用ポリシー（脆弱性の評価基準）」に記載のCVSSの評価に基づき、脆弱性スキャンにて確認された脆弱性情報を示しています。脆弱性が検出された場合は、必要に応じてネットワーク管理者及び各ベンダにご確認ください。なお、深刻度が緊急・重要の脆弱性情報については速やかな対処が必要です。
※早急な対応が必要となる脆弱性が検出された場合、**別紙【脆弱性診断早期報告書】**が作成されます。

脆弱性診断 早期報告　**脆弱性診断早期報告書**

- 貴院の外部ネットワーク接続点における脆弱性診断を実施した結果、
  早急に対応を検討いただきたい事象(※1)が確認されたため、診断結果(簡易版)の早期報告を実施いたします。
  （※1：当社ナレッジから判断して早期報告を実施しています。そのため、脆弱性深刻度が高い脆弱性情報の報告とは限りません。）
- 記載の脆弱性に関する詳細は、後日提出する調査報告書にて確認をお願いします。

早期報告①

概要	脆弱性の影響を受けるソフトウェアを検出		
IPアドレス	36.52.209.88	診断実施日	2025/5/15

バナー情報から脆弱性の影響を受けるバージョンのソフトウェアを利用していることを確認しました。

●OpenSSH_8.5
複数の脆弱性があり、既に攻撃を受け悪用されている可能性があります。
対応をご検討ください。

【脆弱性情報例】
CVE-2024-6387 - OpenSSH 等複数ベンダの製品における競合状態に関する脆弱性
https://jvndb.jvn.jp/ja/contents/2024/JVNDB-2024-004050.html
攻撃コードが公開されています

➢「脆弱性診断早期報告書」は脆弱性診断実施後、1週間後を目安に、ポータルサイトにアップロードされます。
ダウンロード方法はP.3をご確認ください。

参考　脆弱性診断実施条件

脆弱性診断につきまして、以下の条件に当てはまる場合に限り実施いたします。

脆弱性診断 調査希望	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		
調査希望あり	インターネット	固定IP	記入必須	不要	○	
		動的IP	不要	診断実施日（1日目） 連携必須	○	脆弱性診断実施日（1日目）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	記入必須	不要	○	
		動的IP	不要	診断実施日（1日目） 連携必須	○	脆弱性診断実施日（1日目）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	-	-	-	×	
空欄 （調査希望なし）	インターネット インターネット VPN 閉域網	-	-	-	×	

「5.外部ネットワーク接続機器調査」に関して

「5. 外部ネットワーク接続機器調査」に関して

5. 外部ネットワーク接続機器調査

ネットワーク機器調査 1/4

ヒアリングシートにて申告いただいた機器の情報をもとに、調査を実施した結果を記載しています。

申告回線1

機器A

		申告機器No.	機器種別	メーカー	型番	シリアルナンバー
事前申告	機器情報	01A	ファイアウォール/UTM	Fortinet	FortiGate200F	FG200F111111111111

		申告バージョン	最新バージョン	深刻度	緊急	重要	警告	注意
事前申告	脆弱性調査	ファームウェアバージョン 7.6.0	7.6.3F		1件	5件	12件	4件

		桁数	文字混在	ランダムな文字列	定期的な変更	工場出荷時からの変更	異なるパスワードの利用	アカウントの使い分け
事前申告	パスワードポリシー	13桁以上	混在あり	対応あり	7~12か月未満	対応あり	対応あり	対応あり

結果 調査結果

調査機器No. 2

・稼働中のファームウェアバージョンにて脆弱性が確認されました。貴院への影響度合いを確認し、早急にバージョンアップすることをご検討いただくようお願いします。脆弱性情報の詳細は第7章をご確認ください。
・厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合したパスワード管理を実施していることを確認しました。
・アカウント管理について、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合していることを確認しました。

申告回線1

機器B

		申告機器No.	機器種別	メーカー	型番	シリアルナンバー
事前申告	機器情報	01B	ルータ	ヤマハ(YAMAHA)	RTX1300	XXXXXXXXX16

		申告バージョン	最新バージョン	深刻度	緊急	重要	警告	注意
事前申告	脆弱性調査	ファームウェアバージョン 23.00.16	23.00.16		0件	3件	6件	0件

		桁数	文字混在	ランダムな文字列	定期的な変更	工場出荷時からの変更	異なるパスワードの利用	アカウントの使い分け
事前申告	パスワードポリシー	13桁以上	混在あり	対応あり	対応なし	対応あり	対応あり	対応あり

結果 調査結果

調査機器No. 5

・最新ファームウェアバージョンが適用されていますが、既に脆弱性が報告されていますので、メーカーの対応情報を注視してください。脆弱性情報の詳細は第7章をご確認ください。
・厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合したパスワード管理を実施していることを確認しました。
・アカウント管理について、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合していることを確認しました。

※「事前申告」の項目については、ヒアリングシートの記載に基づいて記載しています。

20

補足ポイント

❶申告機器No.

ヒアリングシートの回線情報シートにある「申告機器No.」と照合してご確認ください。

ヒアリングシート　回線情報シート

	機器A（ルータ/ファイアウォール/UTM）											
								パスワードポリシー確認				
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	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
例A	ルータ	シスコシステムズ	ISR 921	ABC1234565N	2A	15.1S	本部棟 3F サーバー室 1番ラック 7U	13桁以上	混在あり	はい	なし	はい
01A	ファイアウォール/UTM	Fortinet	FortiGate200F	FG200F111111111111	4A	7.6.0	3F サーバー室	13桁以上	混在あり	はい	7か月~1年未満	はい

❷ファームウェアバージョン

申告されたメーカー型番に関する最新のファームウェアバージョンを記載しております。
現在稼働中のファームウェアバージョンをご確認のうえ、必要に応じてアップデートをご検討ください。

❸深刻度

巻頭「用語定義・表記凡例・運用ポリシー（脆弱性の評価基準）」に記載のCVSSの評価に基づき、ご利用中のファームウェアバージョンにて確認された脆弱性情報の件数を示しています。脆弱性が検出された場合は、必要に応じてネットワーク管理者及び各ベンダにご確認ください。なお、深刻度が緊急・重要の脆弱性情報については速やかな対処が必要です。
※脆弱性情報の詳細は、**7. 補足資料**に記載しています。

❹パスワードポリシー

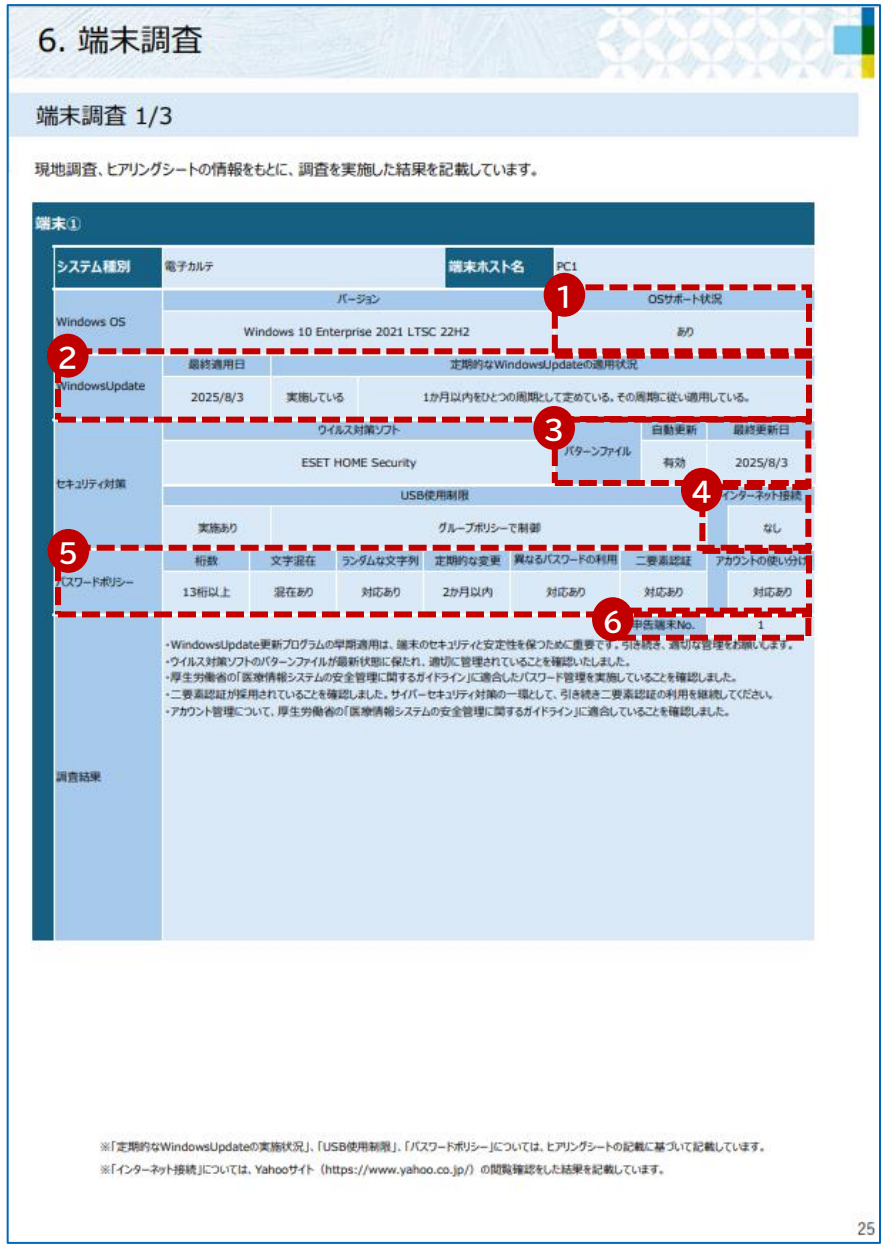
巻頭「用語定義・表記凡例・運用ポリシー（パスワードポリシー）」を参照し、適切に運用できているかご確認ください。

❺調査機器No.

2-2. 現地調査結果一覧にて該当機器をご参照ください。
※現地で確認できなかった機器は「-（ハイフン）」と記載しています。医療機関のネットワークへの影響を考慮し、ケーブルがまとめられている場合や床下配線等で調査が困難である場合、現地で確認作業を実施しておりません。

「6.端末調査」に関して

「6. 端末調査」に関して



6. 端末調査

端末調査 1/3

現地調査、ヒアリングシートの情報をもとに、調査を実施した結果を記載しています。

端末①

システム種別	電子カルテ			端末ホスト名	PC1		
Windows OS	バージョン					OSサポート状況	
	Windows 10 Enterprise 2021 LTSC 22H2					あり	
WindowsUpdate	最終適用日	定期的なWindowsUpdateの適用状況					
	2025/8/3	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。				
セキュリティ対策	ウイルス対策ソフト					自動更新	最終更新日
	ESET HOME Security				パターンファイル	有効	2025/8/3
	USB使用制限					インターネット接続	
	実施あり	グループポリシーで制御				なし	
パスワードポリシー	桁数	文字混在	ランダムな文字列	定期的な変更	異なるパスワードの利用	二要素認証	アカウントの使い分け
	13桁以上	混在あり	対応あり	2か月以内	対応あり	対応あり	対応あり
						申告端末No.	1

調査結果

・WindowsUpdate更新プログラムの早期適用は、端末のセキュリティと安定性を保つために重要です。引き続き、適切な管理をお願いします。
・ウイルス対策ソフトのパターンファイルが最新状態に保たれ、適切に管理されていることを確認いたしました。
・厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合したパスワード管理を実施していることを確認しました。
・二要素認証が採用されていることを確認しました。サイバーセキュリティ対策の一環として、引き続き二要素認証の利用を継続してください。
・アカウント管理について、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合していることを確認しました。

※「定期的なWindowsUpdateの実施状況」、「USB使用制限」、「パスワードポリシー」については、ヒアリングシートの記載に基づいて記載しています。
※「インターネット接続」については、Yahooサイト（https://www.yahoo.co.jp/）の閲覧確認をした結果を記載しています。

25

補足ポイント

❶OSサポート状況
現地で端末OSを確認できた場合、サポート状況の有無を調査いたします。

❷WindowsUpdate
最終更新日には、現地調査で確認できた直近のWindows Update実施日が記載されます。
貴院の把握している実施日と合っているかご確認をお願いいたします。
巻頭「用語定義・表記凡例・運用ポリシー（WindowsUpdate運用ポリシー）」を参照し、適切に運用・管理ができているかご確認ください。

❸パターンファイル
パターンファイルとは、ウイルス対策ソフトが使用する「ウイルス定義ファイル」のことです。
これが最新でないと、ファイルにリストアップされていない新しいウィルスに対応できない可能性があります。
現地でパターンファイルの調査ができた場合、自動更新機能の有無と最終更新日が記載されます。

❹インターネット接続
外部サイトの閲覧可否について記載しております。
必要のないサイトへのアクセスを制限することで、セキュリティインシデントの発生を抑制できます。

❺パスワードポリシー
巻頭「用語定義・表記凡例・運用ポリシー（パスワードポリシー）」を参照し、適切に運用・管理ができているかご確認ください。

❻申告端末No.
ヒアリングシートにて申告いただいた端末の調査ができた場合、申告端末No.が記載されます。現地にて新たにご案内いただいた端末については「-（ハイフン）」が記載されます。

「7.補足資料」に関して

「7. 補足資料」に関して

7. 補足資料

脆弱性詳細情報一覧 1/5

ヒアリングシートにて申告いただいたファームウェアバージョン情報について、確認できた脆弱性情報を記載しています。

メーカー・型番	フォーティネット FortiGate200F	ファームウェアバージョン	7.6.0
申告機器No.	01A 04A		

脆弱性番号	CVSS（深刻度）	対象ファームウェアバージョン	概要
CVE-2025-22252	9.0	7.6.0	複数のフォーティネット製品における重要な機能に対する認証の欠如に関する脆弱性
CVE-2024-40591	8.0	7.6.0	不適切な権限管理による権限昇格
CVE-2024-46670	7.5	7.6.0	ipsec ikeでの領域外読み込みに関する脆弱性
CVE-2024-40591	7.2	7.6.0	不適切な特権者管理による権限超越に関する脆弱性
CVE-2024-48884	7.1	7.6.0	csfdデーモンでのディレクトリトラバーサルに関する脆弱性
CVE-2024-48885	7.1	7.6.0	csfdデーモンでのディレクトリトラバーサルに関する脆弱性
CVE-2024-52965	6.8	7.6.0以上 7.6.1未満	API経由のPKIにおいて、無効な証明書で認証が許可される
CVE-2025-53744	6.8		[illegible]な権限割り当ての脆弱性について
CVE-2025-24477	6.7	7.6.0以上 7.6.3未満	ヒープベースのバッファオーバーフローの脆弱性
CVE-2025-24471	6.5	7.6.0以上 7.6.3未満	証明書検証に関する脆弱性
CVE-2025-22254	6.5	7.6.0以上 7.6.1未満	GUIのWebSocketモジュールにおける権限昇格の脆弱性
CVE-2024-54021	6.4	7.6.0	ウェブプロキシのポリシーでのファイルフィルター回避に関する脆弱性
CVE-2024-3596	6.0	7.6.0	RADIUSプロトコルにおけるCVE-2024-3596：無効な応答の偽造が可能な脆弱性
CVE-2024-55599	4.9	7.6.0	DNSタイプ65のリソースレコード要求がDNSフィルターを回避する
CVE-2024-46666	4.8	7.6.0	非確認領域の境界による複数の論理的破綻に関する脆弱性
CVE-2025-25248	4.8	7.6.0以上 7.6.2未満	Security Fabricにおいて認証処理の不備
CVE-2024-50562	4.4	7.6.0	SSL-VPNのクッキーにおけるセッションの有効期限が不十分

---次ページへ続く---

脆弱性情報詳細

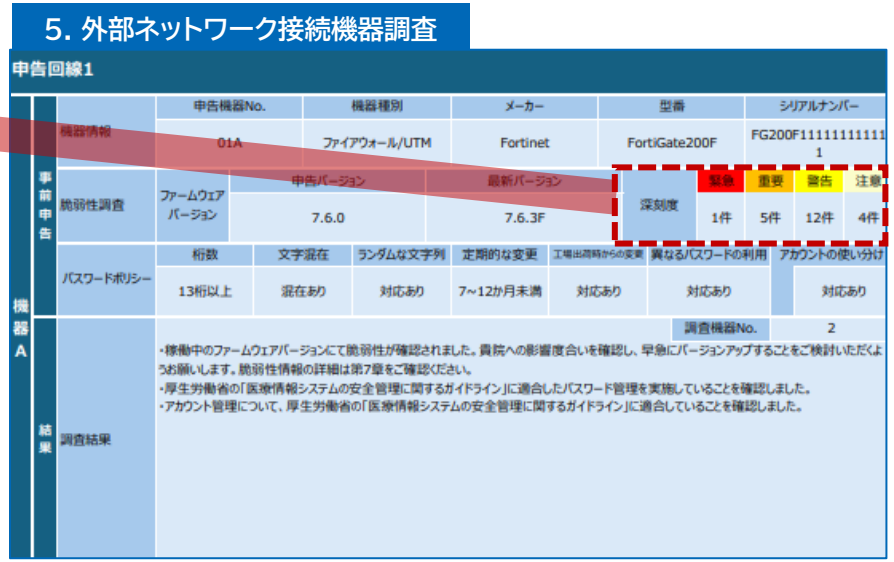
30

補足ポイント

■ヒアリングシートにて申告された現在稼働中のファームウェアバージョンについて、脆弱性情報が確認できた場合、本章に詳細が記載されます。

❶ファームウェアバージョン
申告いただいたファームウェアバージョンが記載されます。

❷脆弱性情報詳細
5. 外部ネットワーク接続機器調査にて確認できた脆弱性情報の詳細を一覧で記載しています。**5. 外部ネットワーク接続機器調査**の調査結果と併せてご確認ください。
※脆弱性番号とは、ソフトウェアやシステムに存在する脆弱性（セキュリティ上の弱点）を識別するために割り当てられる一意の識別子です。次項に記載の「脆弱性データベース」で検索する事で脆弱性情報の詳細が確認可能です。（P.24参照）



5. 外部ネットワーク接続機器調査

申告回線1

		申告機器No.	機器種別	メーカー	型番	シリアルナンバー
機器A	事前申告 機器情報	01A	ファイアウォール/UTM	Fortinet	FortiGate200F	FG200F111111111111

		ファームウェアバージョン	申告バージョン	最新バージョン	深刻度	緊急	重要	警告	注意
機器A	事前申告 脆弱性調査		7.6.0	7.6.3F		1件	5件	12件	4件

		桁数	文字混在	ランダムな文字列	定期的な変更	工場出荷時からの変更	異なるパスワードの利用	アカウントの使い分け
機器A	事前申告 パスワードポリシー	13桁以上	混在あり	対応あり	7~12か月未満	対応あり	対応あり	対応あり

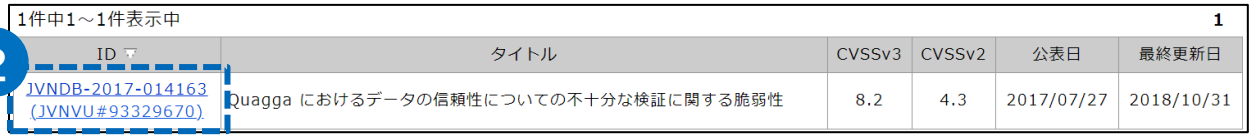
		調査機器No.	2
機器A	結果 調査結果	・稼働中のファームウェアバージョンにて脆弱性が確認されました。貴院への影響度合いを確認し、早急にバージョンアップすることをご検討いただくようお願いします。脆弱性情報の詳細は第7章をご確認ください。 ・厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合したパスワード管理を実施していることを確認しました。 ・アカウント管理について、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に適合していることを確認しました。						

参考　脆弱性データベースにて脆弱性情報を確認する方法

各脆弱性情報について、さらに詳細を確認したい場合、下記の手順でデータベース検索を実施してください。

❶ JVN iPedia - 脆弱性対策情報データベースにて脆弱性番号を検索
❷ ID欄のリンクを押下
❸ 脆弱性情報の詳細、影響、対策方法等が表示されます。影響のある脆弱性かご確認いただき、対応をご検討ください。

➢ 検索対象となる脆弱性番号は**7.補足資料**をご確認ください。



出典: JVN iPedia　https://jvndb.jvn.jp/index.html

地域の価値創造企業へ

SOCIAL INNOVATION パートナー

NTT東日本グループ