NTTサンプル病院 御中

厚生労働省
「令和7年度　医療機関におけるサイバーセキュリティ確保事業」

外部ネットワーク接続点調査報告書

2025/8/22
NTT東日本株式会社

はじめに

目的

「外部ネットワーク接続点調査報告書（本書）」は、
厚生労働省による「令和7年度　医療機関におけるサイバーセキュリティ確保事業」において、
外部ネットワーク接続点の調査として実施した「物理構成の把握」、「ネットワーク機器調査」、「脆弱性診断」、
「端末調査」の結果を総括したものです。

貴院におかれましては、本書を参考に引き続きセキュリティ対策に努めていただくようにお願いします。

全体構成

章番号	タイトル	概要
1	調査結果 総括	全体を総括した報告を実施しています。
2	現地調査結果一覧	現地調査にて確認できた機器一覧、外部ネットワーク接続図、機器設置場所を示した平面図をまとめています。
3	外部ネットワーク接続点の洗い出し・把握	ヒアリングシートの情報をもとに、現地にて調査を実施した結果を記載しています。 ※新規に検出した回線・ネットワーク機器の詳細情報もあわせて記載しています。
4	脆弱性診断	調査対象のグローバルIPアドレスに対してのポートスキャンを行い、インターネットからアクセス可能なポート（サービス）を調査した結果を記載しています。
5	外部ネットワーク接続機器調査	ヒアリングシートの情報をもとに、ネットワーク機器（ルータ/UTM/ファイアウォール）のファームウェアの脆弱性情報の調査、現地での機器の有無を確認した結果を記載しています。
6	端末調査	調査対象の端末に関するセキュリティ対策状況の調査結果を記載しています。
7	補足資料	「5. 外部ネットワーク接続機器調査」において記載している、ヒアリングシートで申告いただいたネットワーク機器のファームウェアバージョンに対し、検出された脆弱性情報の詳細を一覧としてまとめています。

用語定義・表記凡例・運用ポリシー

用語の定義

本資料で使用する用語の定義を以下に示します。

用 語	定 義
申告回線	ヒアリングシートの「申告回線」です。 ヒアリングシートの「申告回線No.」と一致するよう記載しています。
調査回線	現地調査で確認された回線です。 回線の識別のために、「調査回線No.」と記載しています。
申告機器	ヒアリングシートの「装置A」および「装置B」です。 「申告回線No.」と結びつけて、「申告回線No.」+「A」/「B」と記載しています。 （例：01A (申告回線No.01の装置A) ）
調査機器	現地調査で確認された装置です。 確認できた機器ごとに、「調査機器No.」を付与して記載しています。

使用するアイコンの凡例

外部ネットワーク接続図および平面図では、アイコンを用いて外部接続回線およびネットワーク機器を示しています。
それぞれの回線および機器に使用されるアイコンについては、以下をご参照ください。

□回線の凡例

回線No ：調査回線No.
※現地調査時に新規に確認された回線は、「対象外回線」と記載します。

： 有線ケーブル(LANケーブル、光ケーブル、メタルケーブル など)

： 無線通信

□機器の凡例

機器No. ：機器一覧に記載の機器番号

＃〇〇〇 ：ポート番号


回線終端装置
（DSU、モデム など）


ONU内臓ルータ
（TA、VoIPルータ など）


ルータ
（有線・無線含む）


ファイアウォール/UTM


スイッチ
（HUB、給電HUBを含む）


無線AP


端末
（PC/サーバ）


ビジネスホン・PBX主装置

SIM ドングル
SIMドングル

メディアコンバータ
メディアコンバータ

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*）

用語定義・表記凡例・運用ポリシー

WindowsUpdateの運用ポリシー

WindowsUpdateは情報漏洩やサイバー攻撃から守るために非常に重要です。
以下を確認し、適切な対策・管理をお願いします。

WindowsUpdateの主な役割

セキュリティの強化
- マルウェアなどの脅威から保護するセキュリティパッチが提供され、セキュリティ上の脆弱性を修正。

不具合の修正
- OSのバグやエラーを修正し、システムの安定性が向上。

機能の追加・改善
- 新機能の追加や既存機能の改良が行われ、使い勝手が向上。

ドライバーの更新
- 最新のドライバーが提供され、ハードウェアの互換性を確保。

● **WindowsUpdateを適用しない場合のリスク**

セキュリティリスクが増加する

既知の脆弱性が修正されない状態で放置され続けると、ランサムウェアなどシステムの脆弱性を狙ったサイバー攻撃の危険性が高まります。

OS/システムが不安定になる

バグやエラーによって、端末の動作が重い、起動しなくなるなどの不具合は誘発する可能性が高まり、安定的な業務の継続が難しくなる危険性が高まります。

公式のサポートを受けられなくなる可能性が高まる

マイクロソフト社の公式サポートを受けるためには、OSを最新の状態、バージョンにしておく必要があります。

Windows Updateの適切な管理

PC等のOSなどに関する情報は、OSや不正ソフトウェア対策ソフトウェアを提供する事業者などが提供しているほか、重要なセキュリティ関する情報は、「国家サイバー統括室（NCO）」や「独立行政法人 情報処理推進機構(IPA)」などが定期的に公表しています。

これらの情報を確認するほか、必要に応じて利用する情報機器等やソフトウェアを提供する事業者に対応を確認するなどして、最新の情報の入手を図ることが重要です。そのうえで、必要に応じて速やかに脆弱性対策を講じることが求められます。

その際に、他のソフトウェアの動作等に影響することも想定されることから、事前に事業者に脆弱性対策の実施の可否を確認し、対応が難しい場合には、当該リスクに対する対策や管理方法を協議の上、代替策を講じる必要があります。

用語定義・表記凡例・運用ポリシー

パスワードポリシー

ネットワーク機器、PC端末、サーバのパスワードの設定・管理は情報漏洩やサイバー攻撃から守るために非常に重要です。
以下を確認し、適切な対策・管理をお願いします。

1. 推測されやすい文字列のパスワードを利用していると、悪意ある攻撃によってネットワーク内に侵入され、ランサムウェアなどのマルウェアを仕込まれる確率が高まります。

2. 以下において、パスワードに関する望ましい設定が公表されています。
   ①「医療情報システムの安全管理に関するガイドライン　第6.0版（システム運用編）」内の
   「8.利用機器・サービスに対する安全管理措置」
   ②「令和7年度版　医療機関におけるサイバーセキュリティ対策チェックリスト」内の
   「2.医療情報システムの管理・運用」

（１）　情報機器に対して、機器やアプリの起動パスワード等を設定すること。

（２）　設定に当たっては製品等の出荷時におけるパスワードから変更すること。

（３）　推定されにくいパスワードであること。
- a. 英数字、記号を混在させた 13文字以上の推定困難な文字列
- b. 英数字、記号を混在させた8文字以上の推定困難な文字列の定期的な変更
- c. 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列
  ただし他の認証要素として必要な電子証明書等の使用にPIN等が設定されている場合には、この限りではない。
  PCなどの端末については、令和9年度までに二要素認証の実装が求められている。

（４）　利用者や用途によって、アカウント/パスワードを変更すること。

（５）　ネットワーク機器やPC端末、サーバごとに個別のパスワードを設定すること。

1.調査結果　総括

□ 凡例・注記事項

総括表では、「外部ネットワーク接続の俯瞰的把握調査」と「セキュリティ対策等の調査」の2つの観点で、調査結果を件数で表現しています。

「外部ネットワーク接続の俯瞰的把握調査」では、
ヒアリングシートにて申告いただいた情報をもとに実施した現地調査の結果から、申告いただいた情報と差分があった情報をカウントしています。
差分のあった情報については、改めて確認いただき、管理下に置いていただけますようお願いします。

「セキュリティ対策等の調査」では、申告いただいた情報、脆弱性診断等の調査結果から、対応を検討いただきたい事項をカウントしています。
安全性の向上のため、カウントされている項目については、対応を検討いただきますようお願いします。

総括表の項目内容について、以下をご確認ください。

本紙1章

・外部ネットワーク接続の俯瞰的把握

調査項目			
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		
	現地調査で照合できたネットワーク機器	8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	1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	2	
	新規検出回線配下で新規検出された機器		

※「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
※「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

事前申告情報との不一致により、現地調査にて確認できなかったネットワーク機器の件数を示しています。

新規に検出した回線・ネットワーク機器の詳細情報については、「3. 外部ネットワーク接続点の洗い出し・把握」をご参照ください。

・セキュリティ対策等の調査

調査項目			
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		
端末セキュリティ対策	調査端末		
	OSサポートなし		
	セキュリティ対策ソフトなし		
	USB使用制限なし		
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	

申告いただいたグローバルIPアドレスに対して脆弱性診断を実施し、脆弱性が検出されたアドレスの数を示しています。脆弱性の深刻度にかかわらず、脆弱性が検出されたグローバルIPアドレス数を集計しています。(CVSS値が発表されている脆弱性に該当するグローバルIPアドレスが対象)

外部ネットワーク接続機器において、ヒアリングシートに記入いただいたファームウェアバージョンから脆弱性情報の確認ができた装置の台数を示しています。(CVSS値が発表されている脆弱性に該当する装置が対象)

端末調査のパスワードポリシーの件数には、事前申告いただいた電子カルテサーバーのパスワードポリシー情報も含まれています。

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。

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

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。

1-2. 調査結果 総括文言

調査結果　総括文言 2/2

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

端末セキュリティ対策

「端末セキュリティ対策」の調査の結果、OSサポート状況が確認できない端末がありました。正確なOSバージョンを確認いただきOSサポートが終了している場合は、セキュリティパッチが提供されない可能性もあるため、OSのアップグレードをご検討ください。
また、セキュリティ対策ソフトの導入状況が確認できない端末がありました。端末の導入状況を確認いただき未導入の場合は、リアルタイムでの脅威検知や防御など、OSのセキュリティパッチだけではカバーしきれない脅威から端末を守るためにも、セキュリティ対策ソフトの導入をご検討ください。
USB使用制限を実施していない端末も存在しているようです。外部接続媒体を介してマルウェア感染することをありえるため、USB使用制限も合わせてご検討ください。

今後も他の端末を含め、セキュリティを意識した適切な管理をお願いします。調査結果の詳細については、「6. 端末調査」をご確認ください。

パスワードポリシー

「セキュリティ対策等の調査」におけるパスワードポリシーでは、対象機器/端末において、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」に照らし合わせると一部準拠していないパスワードポリシーで運用されている機器/端末があること確認しました。貴院の制約・条件を加味して、ガイドラインに則したパスワードポリシーの運用をご検討ください。また、一部同じアカウントを機器/端末で利用されているようです。異なる用途で同じアカウントやパスワードを使っていると、1つのサービスで情報が漏れた場合、他のサービスにも不正アクセスされるリスクが高まるので、アカウントの使い分けについても、ご検討ください。

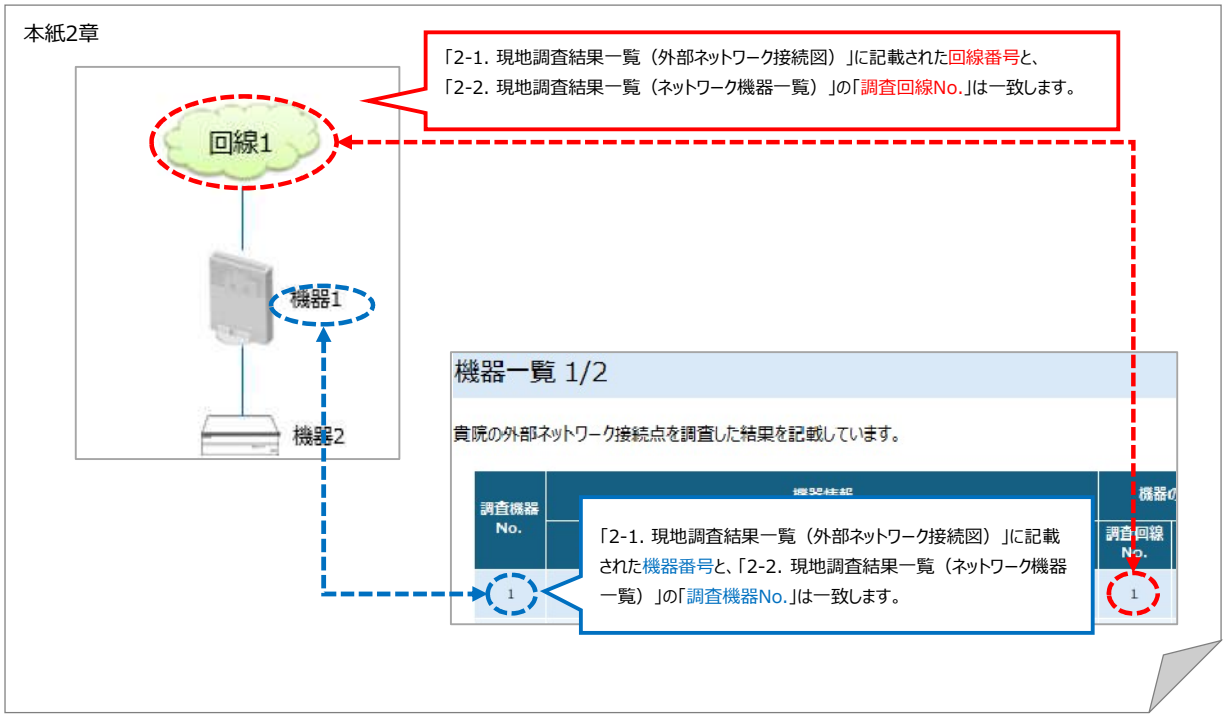
調査結果の詳細については、「5. 外部ネットワーク接続機器調査」、「6. 端末調査」をご確認ください。

2. 現地調査結果一覧

□ 凡例・注記事項

・外部ネットワーク接続図とネットワーク機器の見方

「外部ネットワーク接続図」では、アイコンを用いて外部接続回線およびネットワーク機器を示しています。
それぞれのアイコンに数値を付与し、「ネットワーク機器一覧」と対応させています。



□ 調査未実施の主な理由

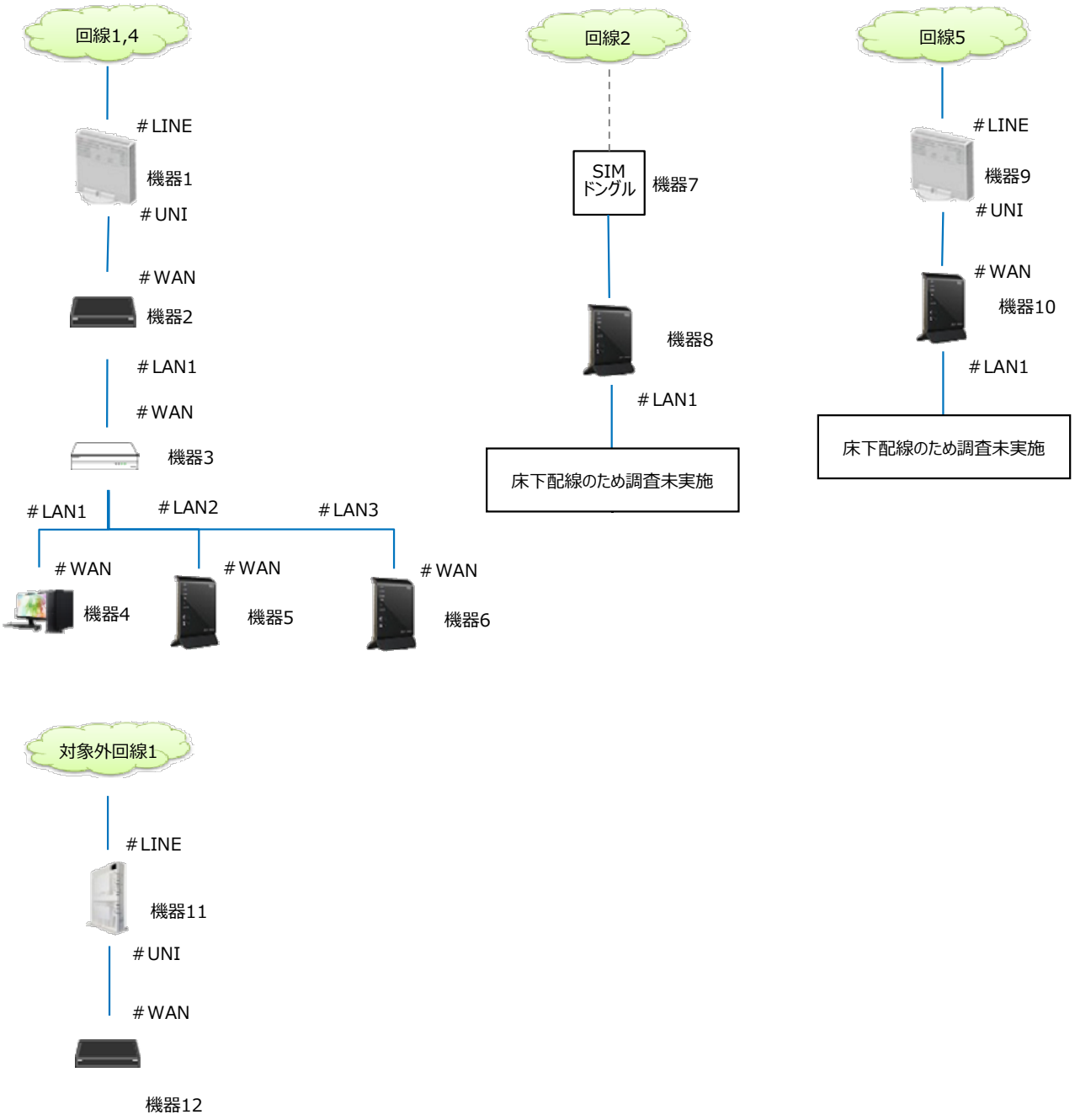
調査が困難であった回線について、外部ネットワーク接続図の一部を作成できない場合があります。
その際、外部ネットワーク接続図上に、調査未実施の理由を記載いたしますので、ご確認ください。
主な理由として、以下のようなものがあります。

・床下配線により、配線が追えない場合
・配線が束ねられている、絡まっている等の理由により、配線が追えない場合
・配線が壁に埋め込まれていることにより、配線が追えない場合
・パッチパネルに接続されており、下部の配線確認が困難な場合

2-1. 現地調査結果一覧（外部ネットワーク接続図）

外部ネットワーク接続図

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。



2-2. 現地調査結果一覧（機器一覧）

機器一覧

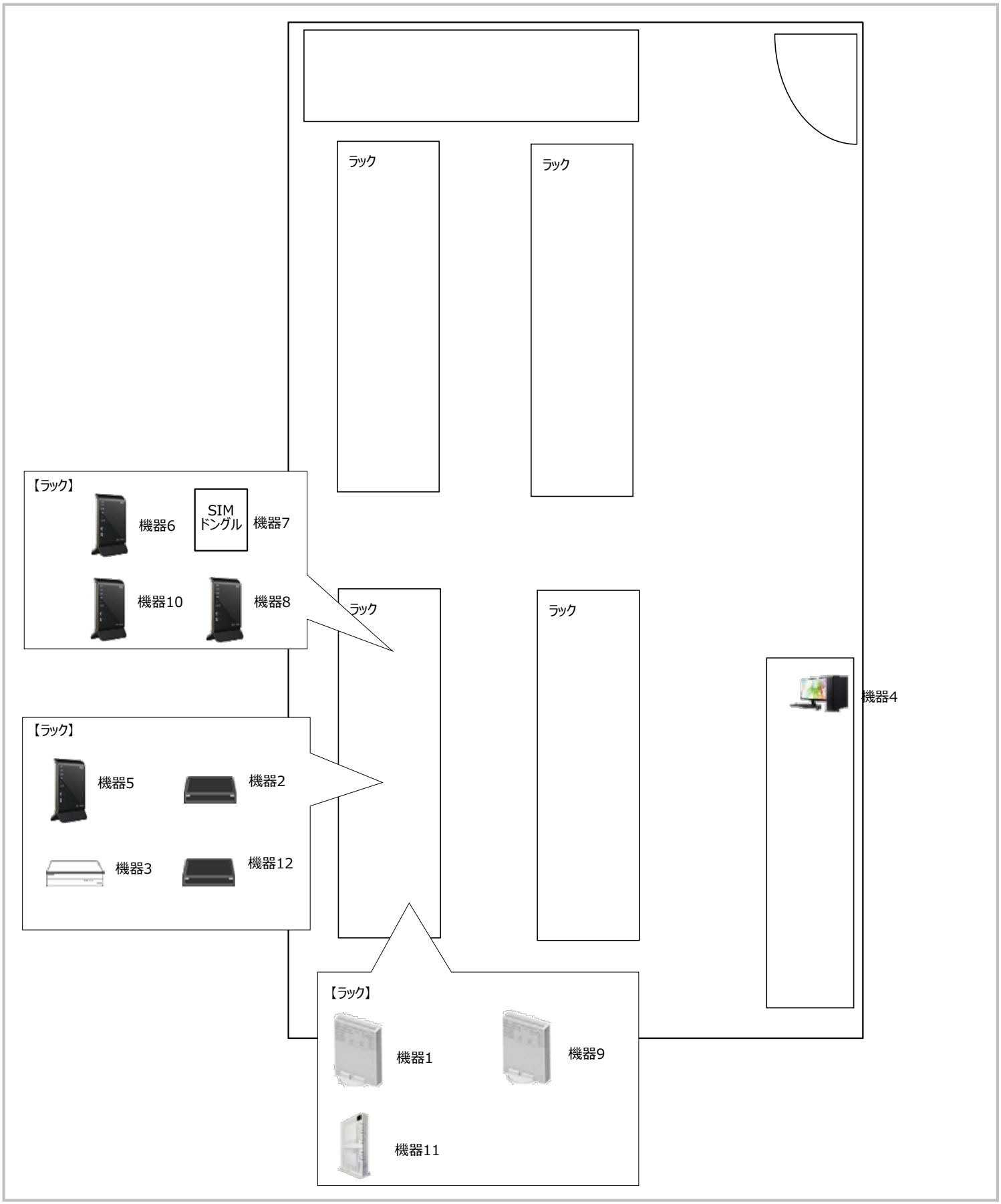
貴院の外部ネットワーク接続点を調査した結果を記載しています。

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	XXXXXXXXXXX22	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						

2-3. 現地調査結果一覧（平面図）

平面図

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。



3. 外部ネットワーク接続点の洗い出し・把握

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。

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 2/2

現地調査にて確認した回線終端装置およびその配下のネットワーク機器を記載しています。
ネットワーク管理者(ベンダ様等)に利用用途をご確認いただき、適切な管理をお願いします。
具体的な配置場所については、「2-3. 現地調査結果一覧（平面図）」にてご確認ください。

<table>
<tr><th>調査回線No.</th><th colspan="7">現地調査結果</th></tr>
<tr><td rowspan="3">対象外回線1</td><td colspan="2">回線終端装置</td><td>調査機器No.</td><td>11</td><td rowspan="3">写真</td><td colspan="2" rowspan="3">  </td></tr>
<tr><td>設置場所</td><td colspan="3">3F サーバ室</td></tr>
<tr><td>回線サービスのID</td><td colspan="3">CAF5555555555</td></tr>
<tr><td rowspan="4">対象外回線1</td><td>ネットワーク機器</td><td>機器A</td><td>調査機器No.</td><td>12</td><td>機器B</td><td>調査機器No.</td><td>-</td></tr>
<tr><td>設置場所</td><td colspan="3">3F サーバ室</td><td>設置場所</td><td colspan="2">-</td></tr>
<tr><td rowspan="2">写真</td><td colspan="3" rowspan="2">  </td><td rowspan="2">写真</td><td colspan="2" rowspan="2">-</td></tr>
<tr></tr>
</table>

外部ネットワーク接続点　調査結果

4. 脆弱性診断

□ 凡例・注記事項

・本章の見方

ヒアリングシート

2. 回線情報

申告回線No.	回線情報				固定IP/動的IP	グローバルIPアドレス	
	回線サービス名	回線サービスのID（CAF番号等）	回線				
例		CAF1111111111	本部棟		固定IP	121.119.249.222	
01		CAF11111111111			固定IP	xxx.xxx.xxx.xxx	

丸数字(緑)
本章の申告回線No.は、ヒアリングシートの申告回線No.と一致します。

丸数字(オレンジ)
本章のIPアドレスは、ヒアリングシートのグローバルIPアドレスと一致します(固定IP)。

本紙4章

申告回線1					
IPアドレス	xxx.xxx.xxx.xxx	脆弱性情報（深刻度）	深刻度レベル	CVSS値	脆弱性番号
応答ポート	23/tcp		警告	5.0	CVE-2025-xxxxx

丸数字(オレンジ)
本章のIPアドレスは、ポータルシステムのグローバルIPアドレスと一致します(固定IP、動的IP)。

ポータルシステム

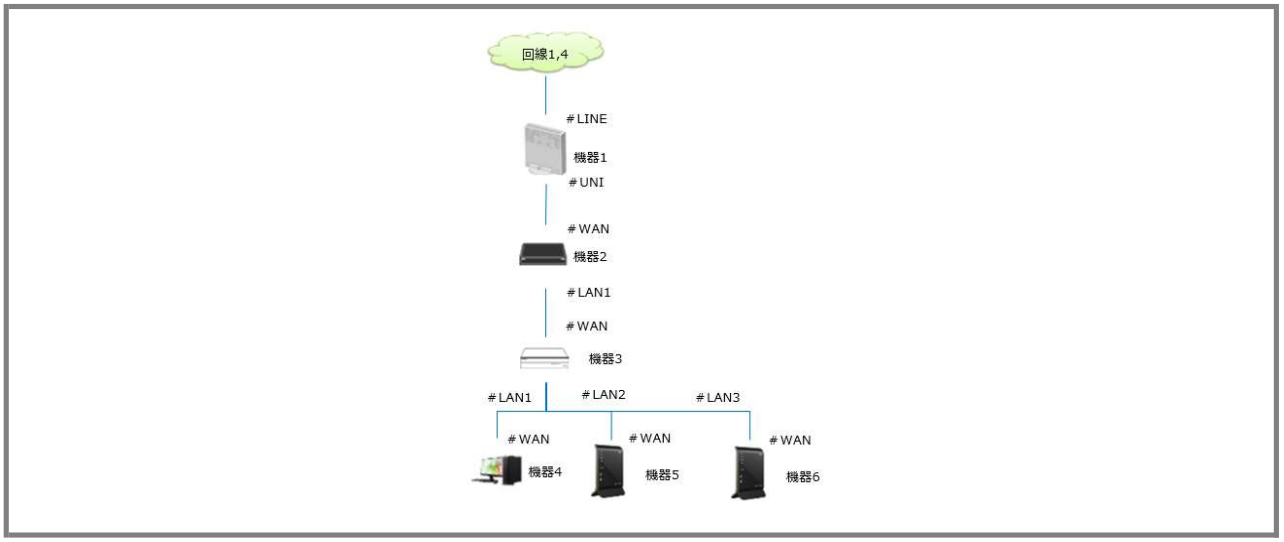
脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	グローバルIPアドレス設定箇所
診断希望あり	インターネット	動的IP	xxx.xxx.xxx.xxx	機器A
診断希望あり	インターネットVPN	固定IP	yyy.yyy.yyy.yyy	機器A

※ポータルシステムは年度内のみ閲覧が可能です。

4. 脆弱性診断

脆弱性診断

貴院の外部ネットワーク接続点に対して脆弱性診断を実施した結果を記載しています。



申告回線1

IPアドレス	111.111.111.111	脆弱性情報（深刻度）	深刻度レベル	CVSS値	CVE番号
応答ポート	123／udp		警告	5.8	なし
調査結果	【ポートスキャン】 ▶NTP サーバーが起動しています。 安全に構成されていない場合は、バージョン、現在の日付、現在の時刻、および場合によってはシステム情報に関する情報が提供される場合があります。 監視、システム運用上、必要な通信ポートであるか確認してください。 【脆弱性スキャン】 ▶NTPサーバがmode6のクエリに応答しています。 特殊なmode6のクエリを攻撃者が投げることによりNTPアンプ攻撃に悪用されてしまう場合があります。 mode6のクエリを信頼できるネットワーク以外から受け付けないように設定してください。				

5. 外部ネットワーク接続機器調査

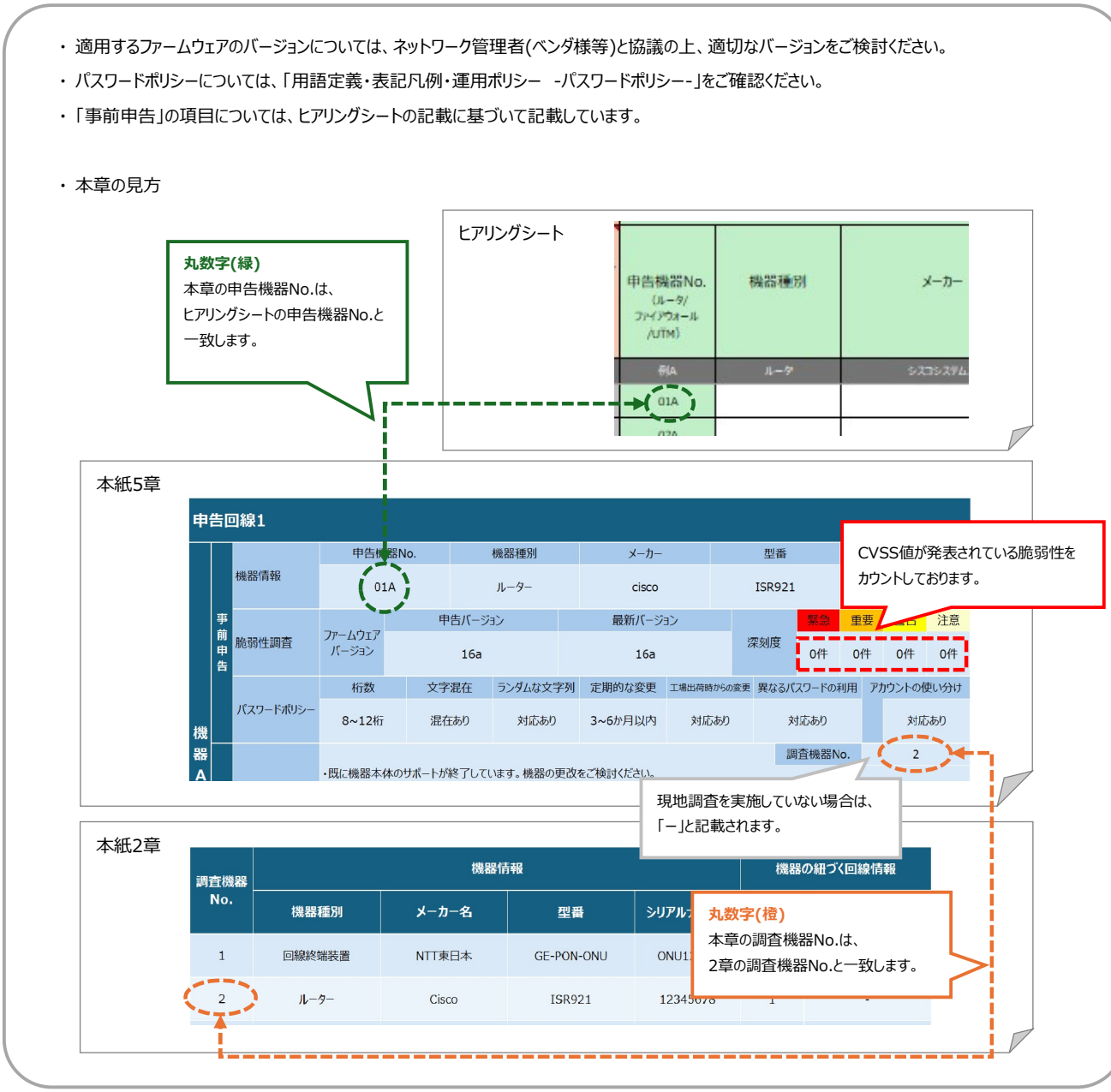
□ 凡例・注記事項

・適用するファームウェアのバージョンについては、ネットワーク管理者(ベンダ様等)と協議の上、適切なバージョンをご検討ください。

・パスワードポリシーについては、「用語定義・表記凡例・運用ポリシー　-パスワードポリシー-」をご確認ください。

・「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。

・本章の見方



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

事前申告

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

脆弱性調査	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
		7.6.0	7.6.3F		1件	5件	12件	4件

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	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
	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。また、機器の環境によって脆弱性への対処が変わる場合がございますので、該当機器の管理者(ベンダー等)にご確認の上、対処方法をご検討ください。
・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

事前申告

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

脆弱性調査	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
		23.00.16	23.00.16		0件	3件	6件	0件

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	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
	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。また、機器の環境によって脆弱性への対処が変わる場合がございますので、該当機器の管理者(ベンダー等)にご確認の上、対処方法をご検討ください。
・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。

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 2/4

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2

機器A	事前申告	機器情報	申告機器No.	機器種別	メーカー	型番	シリアルナンバー					
			02A	ルータ	YAMAHA	RTX830	XXXXXXXXX28					
		脆弱性調査	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		
				15.02.17	15.02.31		0件	4件	6件	1件		
		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	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			
			8~12桁	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.	8								
			・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。また、機器の環境によって脆弱性への対処が変わる場合がございますので、該当機器の管理者(ベンダー等)にご確認の上、対処方法をご検討ください。 ・厚生労働省「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、桁数に応じたパスワードの定期的な変更を推奨しております。「記述基準・表記凡例・調査指針」を参照し、パスワードの変更をご検討ください。 ・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。									

申告回線3

機器A	事前申告	機器情報	申告機器No.	機器種別	メーカー	型番	シリアルナンバー					
			03A	ファイアウォール/UTM	Fortinet	FortiGate100F	FG100F222222222222					
		脆弱性調査	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		
				不明	7.6.3F		-	-	-	-		
		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	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			
			8桁未満	混在なし	対応なし	3~6か月以内	対応あり	対応あり	対応あり			
	結果	調査結果	調査機器No.	-								
			・稼働中のファームウェアバージョンをご確認いただき、最新バージョンにアップデートすることをご検討ください。 ・厚生労働省「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、桁数に応じたパスワードの定期的な変更を推奨しております。「記述基準・表記凡例・調査指針」を参照し、パスワードの変更をご検討ください。 ・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。									

※「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。

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 3/4

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3

機器B

事前申告

機器情報	申告機器No.	機器種別	メーカー	型番	シリアルナンバー
	03B	ルータ	日本電気(NEC)	UNIVERGE WA2105	XXXXXX11

脆弱性調査	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
		10.2.42	-		-	-	-	-

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	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
	不明	不明	不明	不明	不明	不明	不明

結果

調査結果	調査機器No.	-

・貴院より事前申告いただいたメーカー/型番に該当する製品の公開情報が確認できませんでした。
・厚生労働省「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、工場出荷時のパスワード変更、桁数に応じたパスワードの定期的な変更を推奨しております。「記述基準・表記凡例・調査指針」を参照し、パスワードの変更をご検討ください。
・状況や目的に応じて権限を制限したアカウントを準備し、利用者や用途によって、アカウントを使い分けることで、セキュリティインシデント発生時の影響範囲の限定化が期待できます。貴院における運用との兼ね合いを考慮しつつ、アカウントの使い分けをご検討ください。

申告回線4

機器A

事前申告

機器情報	申告機器No.	機器種別	メーカー	型番	シリアルナンバー
	04A	ファイアウォール/UTM	Fortinet	FortiGate200F	FG200F111111111111

脆弱性調査	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
		7.6.0	7.6.3F		0件	0件	2件	0件

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	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
	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。また、機器の環境によって脆弱性への対処が変わる場合がございますので、該当機器の管理者(ベンダー等)にご確認の上、対処方法をご検討ください。
・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。

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 4/4

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4

機器B

事前申告

機器情報	申告機器No.	機器種別	メーカー	型番	シリアルナンバー
	04B	ルータ	ヤマハ(YAMAHA)	RTX1210	XXXXXXXXX30

脆弱性調査	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
		14.01.42	14.01.42		0件	5件	5件	0件

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	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
	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.	6

・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。また、機器の環境によって脆弱性への対処が変わる場合がございますので、該当機器の管理者(ベンダー等)にご確認の上、対処方法をご検討ください。
・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。

6. 端末調査

□ 凡例・注記事項

・Windows OSのサポート状況はマイクロソフト社の以下のサイトを参考にしています。
https://learn.microsoft.com/ja-jp/lifecycle/products/

・パスワードポリシーについては、「用語定義・表記凡例・運用ポリシー　-パスワードポリシー-」をご確認ください。
・「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。

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					
	2025/7/21	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			パターンファイル	自動更新	最終更新日	
	ESET HOME Security				有効	2025/7/21	
	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
調査結果						申告端末No.	1
	・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の適用状況」、「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。

6. 端末調査

端末調査 2/3

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②

システム種別	放射線検査	**端末ホスト名**	HOST-2

Windows OS	バージョン	OSサポート状況
	Windows 11 IoT Enterprise 24H2	あり

WindowsUpdate	最終適用日	定期的なWindowsUpdateの適用状況	
	2025/7/21	-	-

セキュリティ対策	ウイルス対策ソフト	パターンファイル	自動更新	最終更新日
	Microsoft defender(Windows defender)		無効	2023/1/1
	USB使用制限			インターネット接続
	-	-		あり

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
	-	-	-	-	-	-	-

調査結果		申告端末No.	-

・直近での品質更新プログラムの適用が確認できております。改めてWindowsUpdateの適用状況についてご確認ください。
・WindowsUpdate更新プログラムの適用は、端末のセキュリティと安定性を保つために重要です。品質更新プログラムは月に1回の頻度でリリースされますので、リリースタイミングに合わせた定期的な適用の実施をご検討ください。
・ウイルス対策ソフトのパターンファイルにおける自動更新機能が無効となっております。ウイルス対策ソフトのパターンファイルを常に最新状態に保つことで、セキュリティリスクの軽減が期待できます。
・調査実施時点で、[ウイルスと脅威の保護]における警告マークが黄色となっていました。セキュリティ設定を確認し、警告のある項目への対応についてご検討ください。
・USBの使用制限の実施有無を確認できておりません。外部媒体を介してマルウェアに感染するケースも報告されています。USBの使用制限が実施されているか、確認をお願いします。
・厚生労働省「医療情報システムの安全管理に関するガイドライン」に照らし合わせると一部準拠していないポリシーがあります。 次の項目の見直しをお願いします。【桁数、定期的な変更、文字混在、ランダムな文字列、異なるパスワードの利用】
・二要素認証またはこれに相当する対応を行うことを求められています。令和9年度時点で稼働していることが想定される端末の場合、計画的な二要素認証の導入をご検討ください。
・状況や目的に応じて権限を制限したアカウントを準備し、利用者や用途によって、アカウントを使い分けることで、セキュリティインシデント発生時の影響範囲の限定化が期待できます。貴院における運用との兼ね合いを考慮しつつ、アカウントの使い分けをご検討ください。

※「定期的なWindowsUpdateの適用状況」、「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。

6. 端末調査

端末調査 3/3

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③

システム種別	薬剤			**端末ホスト名**	HOST-1		
Windows OS	バージョン				OSサポート状況		
	Windows11				-		
WindowsUpdate	最終適用日	定期的なWindowsUpdateの適用状況					
	-	実施していない	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				
セキュリティ対策	ウイルス対策ソフト			パターンファイル	自動更新	最終更新日	
	-				-	-	
	USB使用制限				インターネット接続		
	実施なし	-				-	
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
	8~12桁	混在なし	対応なし	不定期	対応あり	対応なし	対応なし
調査結果						申告端末No.	2
	・詳細なWindows バージョンが特定できていないため、OSのサポート状況が確認できておりません。詳細なバージョンを把握し、サポートの有無をご確認ください。 ・WindowsUpdate更新プログラムが早期に適用されていない場合、セキュリティホールが残存する状態となります。品質更新プログラムは月に1回の頻度でリリースされます。リリースタイミングに合わせた定期的な適用の実施のため、システム停止を伴う運用計画をご検討ください。 ・ウイルス対策ソフトの確認ができておりません。ウイルス対策ソフトの導入を確認し、適切に管理を実施してください。 ・USBの使用制限を実施していないようです。外部媒体を介してマルウェアに感染するケースも報告されているので、USBの使用制限についてご検討ください。 ・厚生労働省「医療情報システムの安全管理に関するガイドライン」に照らし合わせると一部準拠していないポリシーがあります。 次の項目の見直しをお願いします。【桁数、定期的な変更、文字混在、ランダムな文字列】 ・二要素認証またはこれに相当する対応を行うことを求められています。令和9年度時点で稼働していることが想定される端末の場合、計画的な二要素認証の導入をご検討ください。 ・状況や目的に応じて権限を制限したアカウントを準備し、利用者や用途によって、アカウントを使い分けることで、セキュリティインシデント発生時の影響範囲の限定化が期待できます。貴院における運用との兼ね合いを考慮しつつ、アカウントの使い分けをご検討ください。						

※「定期的なWindowsUpdateの適用状況」、「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。

6. 端末調査

電子カルテサーバ調査

ヒアリングシートにて申告いただいた電子カルテサーバの情報をもとに、パスワードポリシーの結果を記載しています。
なお、電子カルテサーバは事前申告のみで、現地調査は実施しておりません。

電子カルテ サーバ

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
	8~12桁	混在あり	対応あり	3~6か月以内	対応あり	対応あり	対応あり
調査結果	・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。						

※「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。

7. 補足資料

□ 凡例・注記事項

・ 本章は「5. 外部ネットワーク接続機器調査」の補足資料となります。

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	7.6.0以上 7.6.2未満	Security Fabricの構成に関連する不適切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---

7. 補足資料

脆弱性詳細情報一覧 2/5

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。

---前ページの続き---

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	7.6.2

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-2025-24477	4.0	7.6.0以上 7.6.2未満	FortiOS cw_stadデーモンのヒープベースのバッファオーバーフローの脆弱性
CVE-2025-25250	3.9	7.6.0	SSLVPNエンドポイントにおける情報漏洩
CVE-2024-52963	3.5	7.6.0	Ipsecデーモンでの領域外書き込みに関する脆弱性
CVE-2024-46665	3.5	7.6.0	RADIUS認証依頼時の機密情報漏洩に関する脆弱性
CVE-2025-22251	3.0	7.6.0	FGSPにおけるファイアウォールセッションのインジェクション

7. 補足資料

脆弱性詳細情報一覧 3/5

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	ヤマハ　RTX1300	ファームウェアバージョン	23.00.16

申告機器No.	01B

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-2016-2183	7.5	-	「OpenSSL の複数の脆弱性」について
CVE-2006-2007	7.5	-	Winny検出・遮断機能(Winny フィルタ)について
CVE-2018-5389	7.4	-	「IKEv1 のメインモードに総当たり攻撃に対する脆弱性」について
CVE-2005-0039	6.4	23.00.16以下	IPSec 通信の設定に存在する脆弱性
CVE-2017-3224	5.8	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について
CVE-2017-3752	5.8	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について
CVE-2017-6770	5.8	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について
CVE-2004-2761	5.0	-	MD5アルゴリズムの脆弱性について
CVE-2008-1654	4.3	-	UPnP機能に関する脆弱性について

7. 補足資料

脆弱性詳細情報一覧 4/5

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	ヤマハ RTX830	ファームウェアバージョン	15.02.17

申告機器No.	02A

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-2017-3752	8.2	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性
CVE-2017-3224	8.2	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性
CVE-2016-2183	7.5	-	TLS プロトコルなどの製品で使用される DES および Triple DES 暗号における平文のデータを取得される脆弱性
CVE-2018-5389	7.4	-	IKEv1 のメインモードに総当たり攻撃に対する脆弱性
CVE-2005-0039	6.4	-	IPsecのESPトンネルモードに関する脆弱性
CVE-2004-2761	5.0	-	MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造
CVE-2021-20843	4.8	15.02.17以前	クロスサイトスクリプトインクルージョン
CVE-2008-1654	4.3	-	UPnP が有効になっている場合の問題
JVNVU#99671861	4.3	-	UPnP を実装した複数のルータ製品にセキュリティ機能の実装が不十分な問題
CVE-2017-6770	4.2	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について
CVE-2021-20844	3.7	15.02.17以前	HTTP レスポンスヘッダインジェクション

7. 補足資料

脆弱性詳細情報一覧 5/5

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	ヤマハ RTX1210	ファームウェアバージョン	14.01.42

申告機器No.	04B

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-2017-3752	8.2	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性
JVNVU#91475438	7.8	-	IKE/IKEv2プロトコルがDOS攻撃に悪用される脆弱性
CVE-2016-2183	7.5	-	TLS プロトコルなどの製品で使用される DES および Triple DES 暗号における平文のデータを取得される脆弱性
CVE-2006-2007	7.5	-	Winny検出・遮断機能(Winny フィルタ)について
CVE-2018-5389	7.4	-	IKEv1 のメインモードに総当たり攻撃に対する脆弱性
CVE-2005-0039	6.4	-	IPsecのESPトンネルモードに関する脆弱性
CVE-2004-2761	5.0	-	MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造
CVE-2008-1654	4.3	-	UPnP が有効になっている場合の問題
JVNVU#99671861	4.3	-	UPnP を実装した複数のルータ製品にセキュリティ機能の実装が不十分な問題
CVE-2017-6770	4.2	-	OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について