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「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)

2024年12月

東日本電信電話株式会社　ビジネスイノベーション本部

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」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）

- 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**1か月半～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。

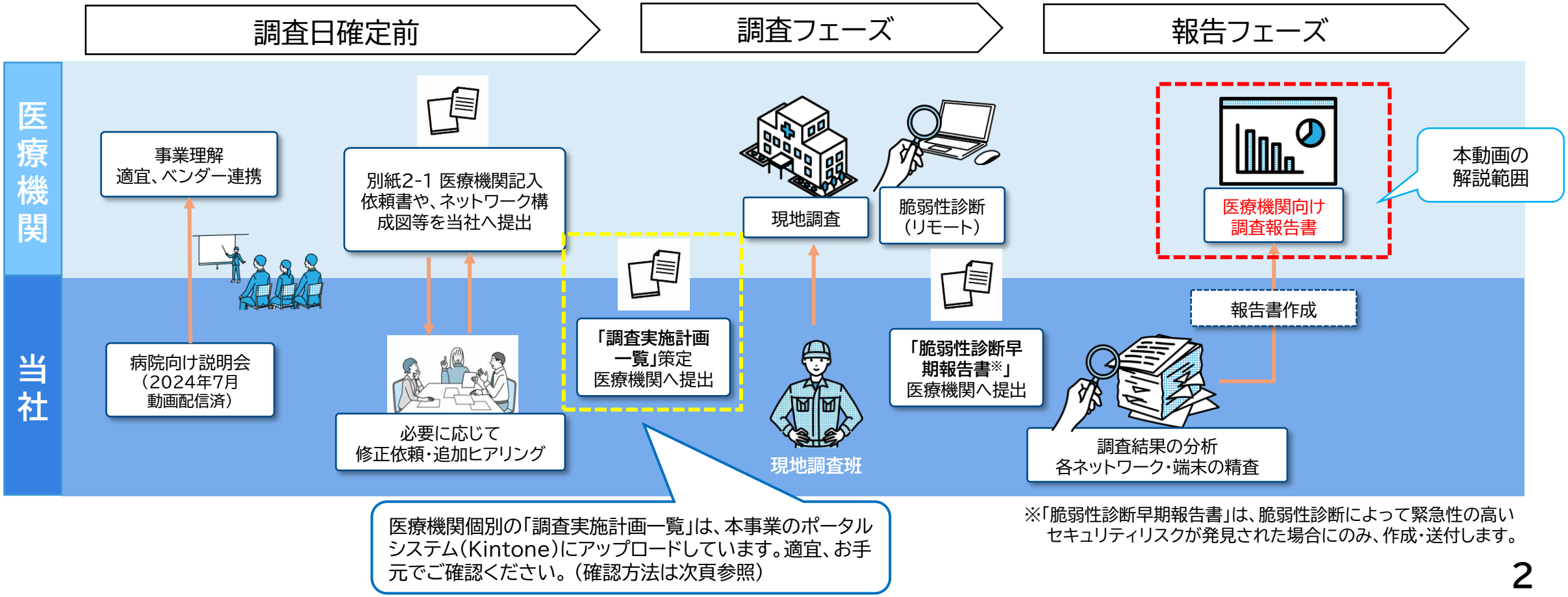
- 事前に以下をお手元にご用意の上、ご視聴下さい。
  ・「外部ネットワーク接続点調査報告書」（以下、**調査報告書**）
  ・「別紙2－1_医療機関記入依頼書（回線・機器情報等記入）」（以下、**医療機関記入依頼書**） ※事前に事務局へ提出したもの
  ・「**調査実施計画一覧**」 ※詳細は次頁をご参照下さい

- 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： 240703 医療機関におけるサイバーセキュリティ確保事業 病院説明会（youtube.com）

■「医療機関向け説明会資料」の掲載場所
・病院説明会動画の下部の概要欄（左図）に医療機関向け説明会資料の本編から別紙1～別紙8まで掲載しております。

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、**当社にて調査範囲・調査対象を記載した「調査実施計画一覧」を作成し、現地調査および脆弱性診断を実施しています**。（「調査実施計画一覧」の取得方法は次頁をご参照下さい）
- 医療機関からご提出いただいた医療機関記入依頼書と調査報告書の回線番号や端末番号に相違が生じる場合があります。ご注意の上、ご確認ください。（詳細はP.8をご参照下さい）



※「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　調査実施計画一覧、調査報告書の取得方法（抜粋）

- 調査実施計画一覧、調査報告書は、**ポータルシステムの「06 情報提供・報告書送付」より取得をお願いします※。**
  ※調査時期によって、ポータルシステム内の「02_ファイル管理」にて提供している場合があります。あわせてご確認下さい。
- 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。

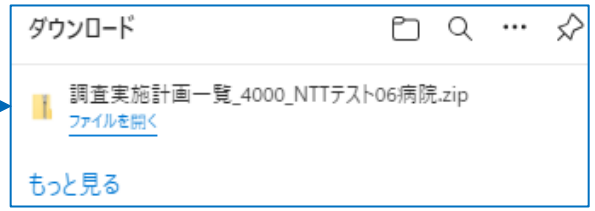
Step 1　資料がアップロードされると、kintone（no-reply@cybozu.com）より病院担当者宛に通知メールが届く

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

Step 2　ポータルシステム（Kintone）内の「06_情報提供・報告書送付」より資料を取得

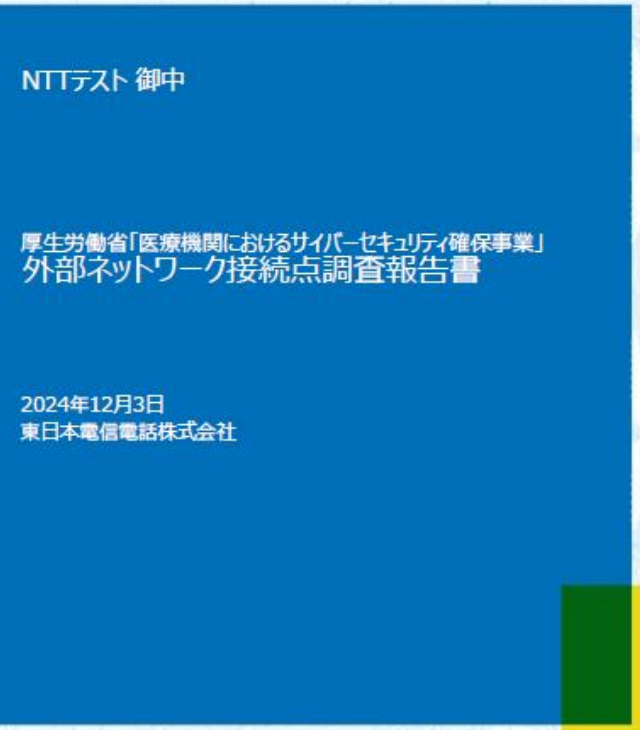
3　ログイン後、自動的に左記の画面に遷移します



- 「調査実施計画一覧」は現地調査日の3～7営業日前を目安にアップロードされます
- 「外部ネットワーク接続点調査報告書」は調査実施後、1.5か月～2か月後を目安にアップロードされます

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

「外部ネットワーク接続点調査報告書」の補足説明



「はじめに・総括」について

「1.外部接続点を中心とした物理構成の把握」について

「2.外部ネットワーク接続機器調査」について

「3.脆弱性診断」について

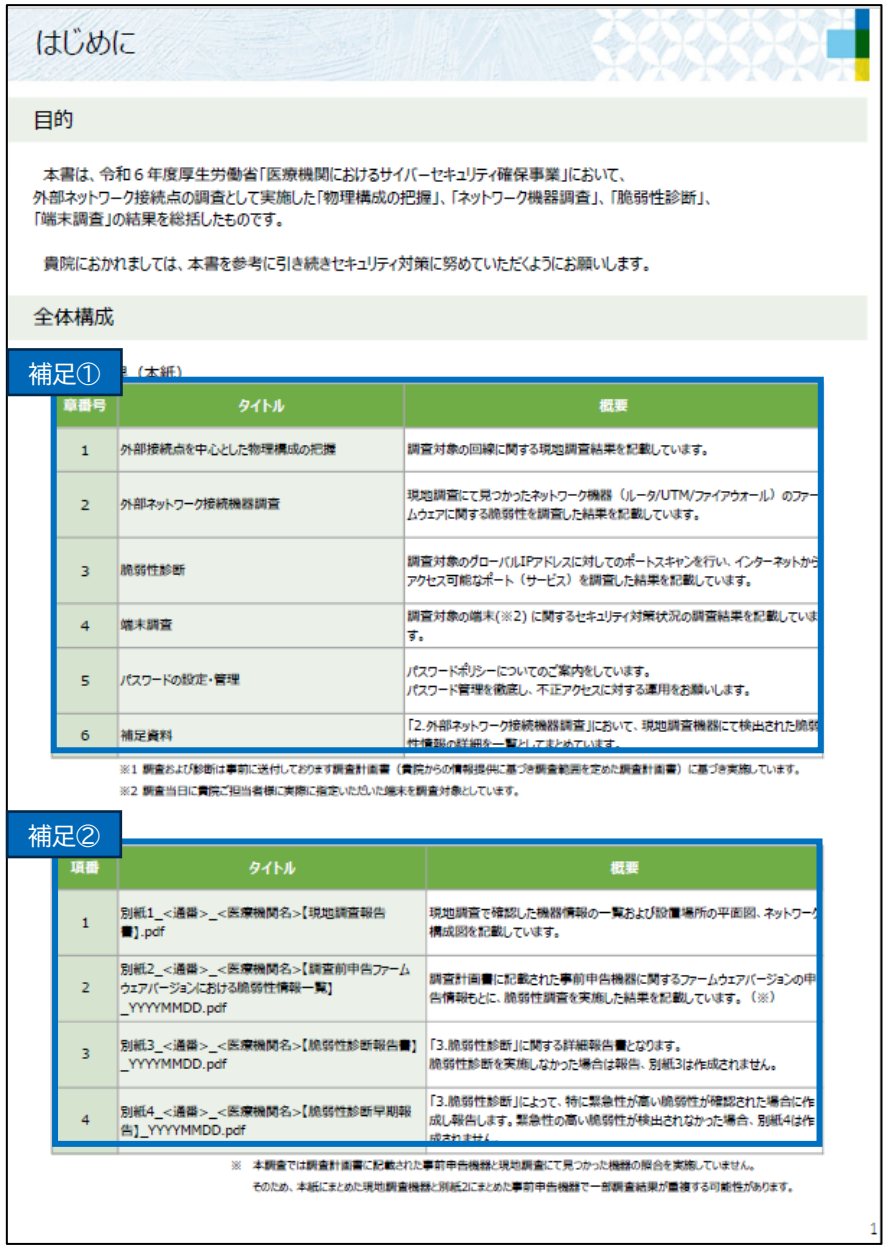
「4.端末調査」について

「5.パスワードの設定・管理」について

「6.補足資料」について

「はじめに・総括」について

「はじめに」に関して



はじめに

目的

本書は、令和６年度厚生労働省「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

補足①

（本紙）

章番号	タイトル	概要
1	外部接続点を中心とした物理構成の把握	調査対象の回線に関する現地調査結果を記載しています。
2	外部ネットワーク接続機器調査	現地調査にて見つかったネットワーク機器（ルータ/UTM/ファイアウォール）のファームウェアに関する脆弱性を調査した結果を記載しています。
3	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。
4	端末調査	調査対象の端末(※2) 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。
5	パスワードの設定・管理	パスワードポリシーについてのご案内をしています。 パスワード管理を徹底し、不正アクセスに対する運用をお願いします。
6	補足資料	「2.外部ネットワーク接続機器調査」において、現地調査機器にて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。

※1 調査および診断は事前に送付しております調査計画書（貴院からの情報提供に基づき調査範囲を定めた調査計画書）に基づき実施しています。
※2 調査当日に貴院ご担当者様に実際に指定いただいた端末を調査対象としています。

補足②

項番	タイトル	概要
1	別紙1_<通番>_<医療機関名>【現地調査報告書】.pdf	現地調査で確認した機器情報の一覧および設置場所の平面図、ネットワーク構成図を記載しています。
2	別紙2_<通番>_<医療機関名>【調査前申告ファームウェアバージョンにおける脆弱性情報一覧】_YYYYMMDD.pdf	調査計画書に記載された事前申告機器に関するファームウェアバージョンの申告情報もとに、脆弱性調査を実施した結果を記載しています。（※）
3	別紙3_<通番>_<医療機関名>【脆弱性診断報告書】_YYYYMMDD.pdf	「3.脆弱性診断」に関する詳細報告書となります。 脆弱性診断を実施しなかった場合は報告、別紙3は作成されません。
4	別紙4_<通番>_<医療機関名>【脆弱性診断早期報告】_YYYYMMDD.pdf	「3.脆弱性診断」によって、特に緊急性が高い脆弱性が確認された場合に作成し報告します。緊急性の高い脆弱性が検出されなかった場合、別紙4は作成されません。

※ 本調査では調査計画書に記載された事前申告機器と現地調査にて見つかった機器の照合を実施していません。
そのため、本紙にまとめた現地調査機器と別紙2にまとめた事前申告機器で一部調査結果が重複する可能性があります。

1

補足①

調査報告書本紙の各章の概要について記載しています。

補足②

調査報告書別紙の概要について記載しています。

■別紙1【現地調査報告書】
現地調査で確認した機器情報の一覧および設置場所の平面図、ネットワーク構成図を記載しています。全体構成の把握にお役立てください。

■別紙2【調査前申告ファームウェアバージョンにおける脆弱性情報一覧】
ご提出いただいた「医療機関記入依頼書」上、ファームウェアバージョンの記載があった機器に関する脆弱性情報を記載しています。「医療機関記入依頼書」、「調査実施計画一覧」と照らし合わせてご確認ください。

■別紙3【脆弱性診断報告書】
「3.脆弱性診断」に関する詳細報告書です。脆弱性の詳細確認や、ネットワーク管理者に脆弱性情報をご報告する際にお役立てください。

■別紙4【脆弱性診断早期報告】
「3.脆弱性診断」にて、特に緊急性が高い脆弱性が確認された場合に作成します。緊急性の高い脆弱性が検出されなかった場合は作成されません。別紙4が作成された場合には、早急な対応を推奨します。

「調査結果　総括」に関して

調査結果 総括

調査実施日

調査実施日	現地調査実施日	2024年12月1日
	脆弱性診断実施日	2024年12月1日
	OS/脆弱性情報確認	2024年11月時点での脆弱性情報を基にしています。

調査結果

現地調査　調査結果（本紙）

章番号		補足	件数
1	外部接続点を中心とした物理構成の把握	調査対象の回線数	7
		現地調査で確認できた回線	6
		現地調査で新規に検出した回線数	1
2	外部ネットワーク接続機器調査	現地調査で確認したネットワーク機器数	7
		脆弱性調査対象(ファームウェアバージョン判明機器)	3
		脆弱性検出あり（※1）	3
3	脆弱性診断	診断対象のグローバルIPアドレス数	3
		脆弱性診断実施	2
		脆弱性検出あり（※2）	1
4	端末調査	調査端末数	5
		OSサポートなし	1
		セキュリティ対策ソフトなし	1

※1 外部回線に接続されているネットワーク機器（ルータ/UTM/ファイアウォール）において、稼働中ファームウェアバージョンから脆弱性情報が検出された装置の台数を示しています。

※2 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。

※3 調査および診断は事前に送付しております調査計画書（貴院からの情報提供に基づき調査範囲を定めた調査計画書）に基づき実施しています。

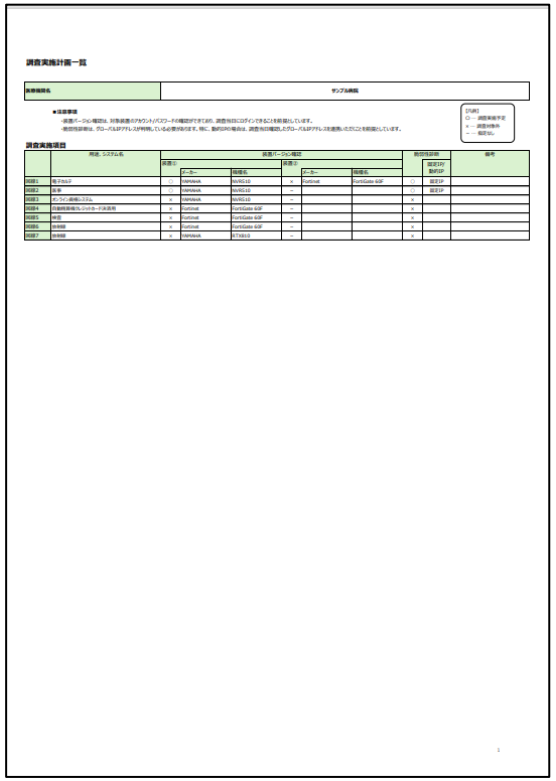
※4 本事業では、脆弱性の評価基準として共通脆弱性評価システムCVSSを採用しています。また、上記表では深刻度のレベルに関わらず、脆弱性が検出された機器およびグローバルIPアドレス数をカウントし、集計しています。

補足

・「調査対象の回線数」は、事前にポータルシステム（kintone）にアップロードした「調査実施計画一覧」に基づいています。

・「現地調査で確認できた回線数」は、調査対象回線※のうち、現地で確認できた数を示しています。（※詳細は次頁をご参照下さい）

「調査実施計画一覧」イメージ



補足　調査対象回線、回線番号の考え方

■医療機関よりご提出いただいた「医療機関記入依頼書」

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 (*)	回線情報					
	装置バージョン確認 (*)	脆弱性診断 (*)		用途、システム名 (*)	回線サービス名	回線ID	回線事業者	回線名義	通信形態 (*)
記入例	調査希望あり	調査希望あり	あり	電子	トタイプ	CAFXXXX	NTT東日本	株式会社XX	インターネットVPN
回線1	調査希望あり	調査希望あり	あり	電子		CAF1234567890AA A	NTT東日本	○×病院	インター
回線2	調査希望あり	調査希望あり	あり			CAF1234567890AA A	NTT東日本	○×病院	インター
回線3	調査希望あり	調査希望あり	なし	薬剤	フレッツ光ネクスト ファミリータイプ	CAF1234567890BB B	NTT東日本	○×病院	インターネット
回線4	調査希望あり	調査希望あり	あり	ナースコール	ISDN	CAF1234567890CC C	NTT東日本	システムベンダー	電話回線のみ
回線5		調査希望なし	あり	オンライン資格システム	フレッツ光ネクスト ファミリータイプ	CAF1234567890DD D	NTT東日本	システムベンダー	インターネット
回線6	調査希	希望あり	あり	自動精算機クレジットカード決済用	フレッツ光ネクスト・ファミリーSHS隼	CAF1234567890EE E	NTT東日本	システムベンダー	インターネットVPN
回線7					LTE閉域回線		NTT	システムベンダー	閉域網
回線8					フレッツ光ネクスト ファミリー・ハイスピードタイプ	CAF1234567890GG G	NTT東日本	システムベンダー	インターネットVPN
回線9					フレッツ光ネクスト ファミリー・ハイスピードタイプ	CAF1234567890HH H	NTT東日本	システムベンダー	

電子カルテシステムの所属するネットワークとの接続「なし」

通信形態「電話回線のみ」

対象外回線を削除
↓
回線番号にズレが生じる

調査対象外回線を削除、回線番号を振り直して、「調査実施計画一覧」に反映

調査実施計画一覧

医療機関名　サンプル

■注意事項
・装置バージョ　提としています。
・脆弱性診断　たグローバルIPアドレスを連携い

医療機関記入依頼書「回線5」が調査実施計画一覧で「回線3」に

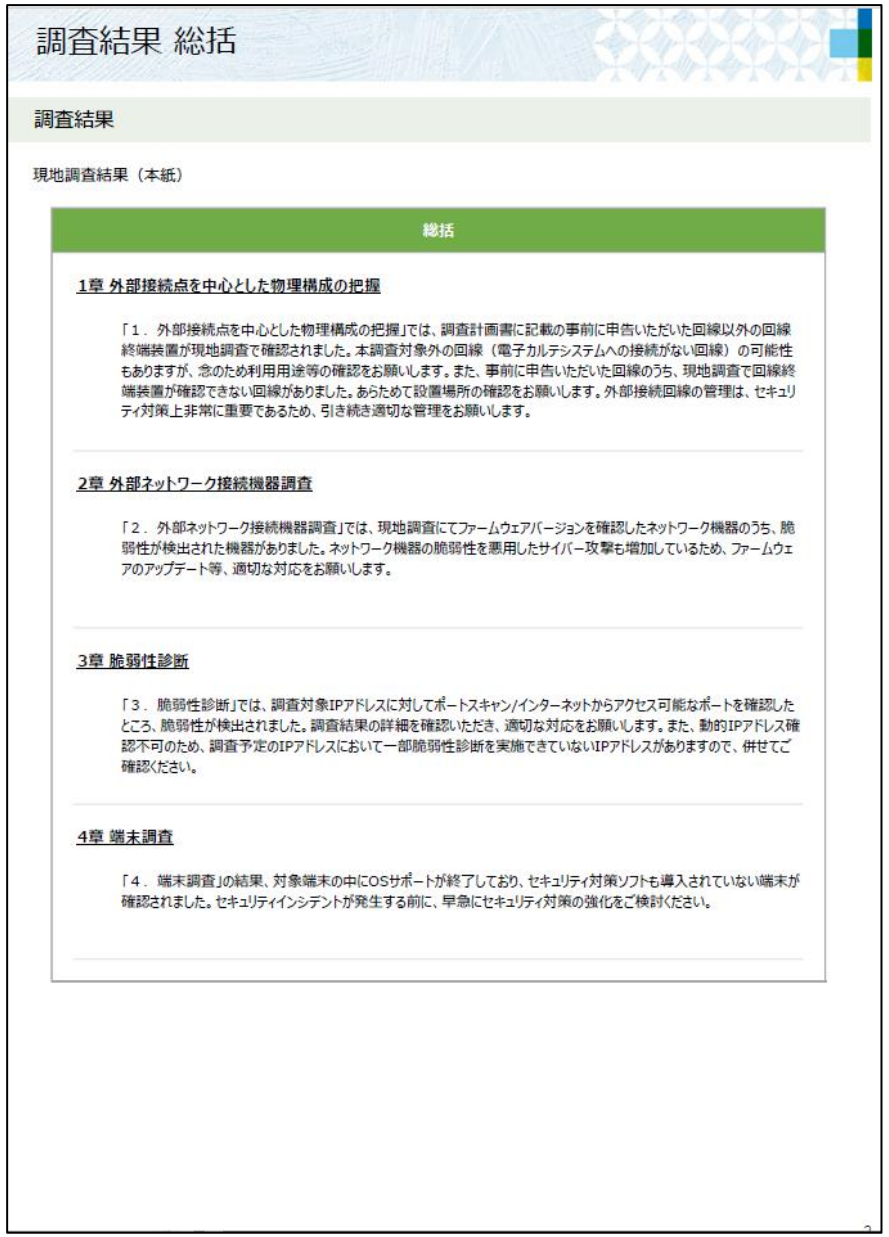
調査実施項目

		ョン確認								
		装置①	メーカー	機種名	装置②	メーカー			固定IP	
回線1	電子カルテ	○	YAMAHA	NVR510	×	Fortinet				
回線2	医事	○	YAMAHA	NVR510	–			○	固定IP	
回線3	オンライン資格システム	×	YAMAHA	NVR510	–			×		
回線4	自動精算機クレジットカード決済用	×	Fortinet	FortiGate 60F	–			×		
回線5	検査	×	Fortinet	FortiGate 60F	–			×		
回線6	放射線	×	Fortinet	FortiGate 60F	–			×		
回線7	放射線	×	YAMAHA	RTX810	–			×		

＜調査対象回線の考え方＞
・調査対象回線は、電子カルテシステムと接続のある回線（電話回線を除く）となります。「調査実施計画一覧」には調査対象回線のみを記載しています。

＜回線番号の考え方＞
・ご提出いただいた「医療機関記入依頼書」に調査対象外回線の記載があった場合には、その回線を除いた上で回線番号を振り直しています。

「調査結果　総括」に関して



調査結果 総括

調査結果

現地調査結果（本紙）

総括

1章 外部接続点を中心とした物理構成の把握

「1．外部接続点を中心とした物理構成の把握」では、調査計画書に記載の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、念のため利用用途等の確認をお願いします。また、事前に申告いただいた回線のうち、現地調査で回線終端装置が確認できない回線がありました。あらためて設置場所の確認をお願いします。外部接続回線の管理は、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。

2章 外部ネットワーク接続機器調査

「2．外部ネットワーク接続機器調査」では、現地調査にてファームウェアバージョンを確認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。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、ファームウェアのアップデート等、適切な対応をお願いします。

3章 脆弱性診断

「3．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、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。また、動的IPアドレス確認不可のため、調査予定のIPアドレスにおいて一部脆弱性診断を実施できていないIPアドレスがありますので、併せてご確認ください。

4章 端末調査

「4．端末調査」の結果、対象端末の中にOSサポートが終了しており、セキュリティ対策ソフトも導入されていない端末が確認されました。セキュリティインシデントが発生する前に、早急にセキュリティ対策の強化をご検討ください。

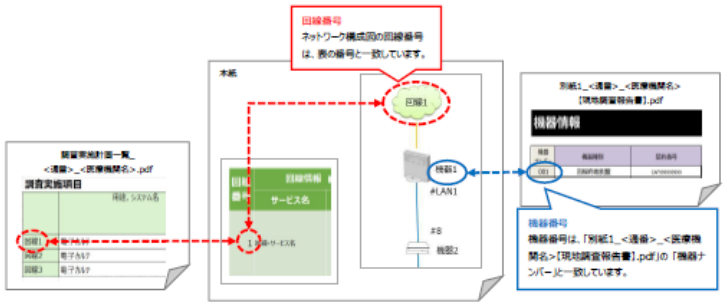
各調査の結果の要約を記載しています。詳細は各章をご確認ください。

「表記について」に関して

表記について

ネットワーク構成図

ネットワーク構成図では、アイコン(※)を用いてネットワーク機器および外部接続回線を示しています。
それぞれの機器アイコンに数値を付与して、ページ内の表・別紙との関連性を示しています。
また、ネットワーク構成図と表は同一ページ内で対応しています。



※ 使用されるアイコンの詳細は「別紙1_<通番>_<医療機関名>【現地調査報告書】.pdf」をご参照ください。

の評価基準

補足

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

・詳細については下記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(PoCやExploitなど)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、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）

4

補足

・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

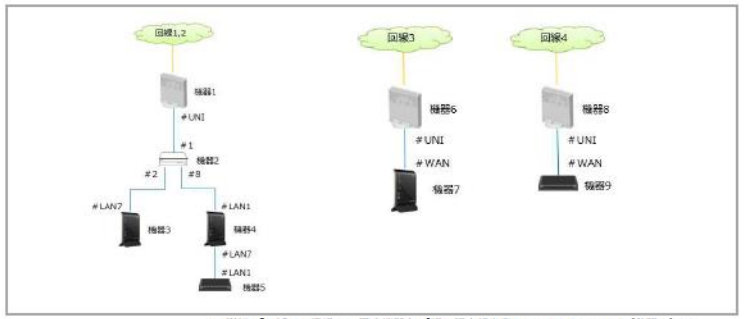
「1. 外部接続点を中心とした物理構成の把握」について

「1. 外部接続点を中心とした物理構成の把握」について

1. 外部接続点を中心とした物理構成の把握 1/3

ネットワーク構成図

貴院の外部ネットワーク接続点における回線を調査した結果は以下の通りです。



※ 詳細は「別紙1_<通番>_<医療機関名>【現地調査報告書】_YYYYMMDD.pdf」をご参照ください。

回線番号	調査計画書記載 事前申告回線				現地調査結果		調査結果
	サービス名	回線ID	用途・システム名	通信形態	差分	回線ID	
1	フレッツ光ネクスト ファミリータイプ	CAF1234567890AAA	自動精算機クレジットカード決済用	インターネット	無	CAF1234567890AAA	事前に提供いただいた情報通りに回線が存在することを現地調査にて確認しています。
2			医事	インターネット	無		事前に提供いただいた情報通りに回線が存在することを現地調査にて確認しています。
3	フレッツ光ネクスト ファミリータイプ	CAF1234567890DDD	オンライン資格システム	インターネット	無	CAF1234567890DDD	事前に提供いただいた情報通りに回線が存在することを現地調査にて確認しています。
4	フレッツ光ネクスト・ファミリーSHS準	CAF1234567890EEE	電子カルテ	インターネットVPN	無	CAF1234567890EEE	事前に提供いただいた情報通りに回線が存在することを現地調査にて確認しています。
5	フレッツ光ネクスト・ファミリーSHS準	CAF1234567890FFF	検査	閉域網	有	不明	現地調査において回線が確認できず、事前に提供いただいた情報通りに回線が存在することを確認できておりません。 ネットワーク管理者(ベンダー等)に確認をお願いします。

補足

補足

・「事前にご提供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、ネットワーク管理者への確認をお願いします。
※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な状況である場合、現地で確認作業を実施していません。

・構成図の表記・凡例につきましては、『別紙1【現地調査報告書】』をご参照ください。

別紙1【現地調査報告書】
現地調査で確認した機器情報の一覧および設置場所の平面図、ネットワーク構成図を記載しています。

補足　回線番号「対象外回線」の記述について

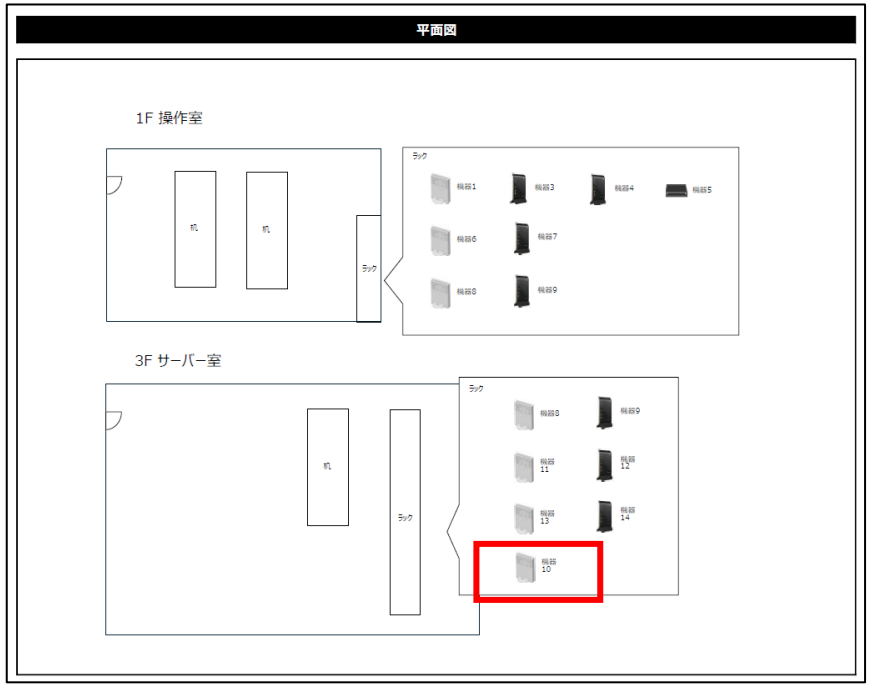
・「医療機関記入依頼書」に記載がなかった回線終端装置が現地で新たに確認された場合、回線番号欄に「対象外回線」と記載しています。

・医療機関で把握されていない回線の場合は、ネットワーク管理者にご確認ください。

・「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」や「電話回線のみの回線」の場合がありますので、ご了承ください。

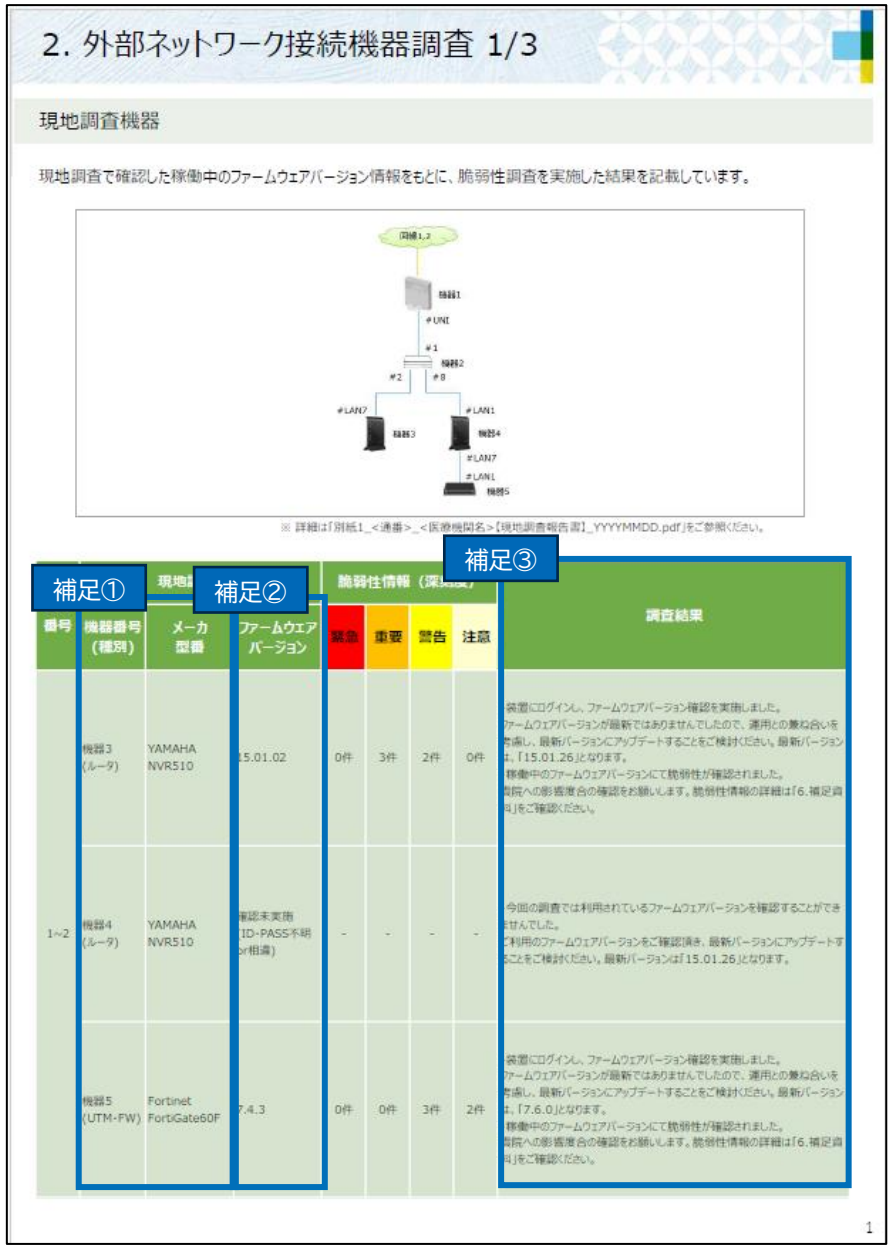
・回線終端装置の設置場所については、別紙1【現地調査報告書】の平面図と照らし合わせてご確認ください。

【例】左のサンプルでは＜機器10＞が該当。
　　⇒別紙1【現地調査報告書】の平面図から＜機器10＞を確認



「2. 外部ネットワーク接続機器調査」について

「2. 外部ネットワーク接続機器調査」について



補足①

・回線IDごとに、現地で確認できた機器を記載しています。
・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いません。なお、現地で確認できなかった機器は記載していません。

補足②

・「現地でログインを実施した機器」のファームウェアバージョンを記載しています。
・現地でログインを実施していない機器は、「確認未実施」と記載しています。
・事前にファームウェアバージョンをご共有いただいた機器については、現地の確認可否に関わらず、『別紙2【調査前申告ファームウェアバージョンにおける脆弱性情報一覧』に記載しています。（次頁で解説）

補足③

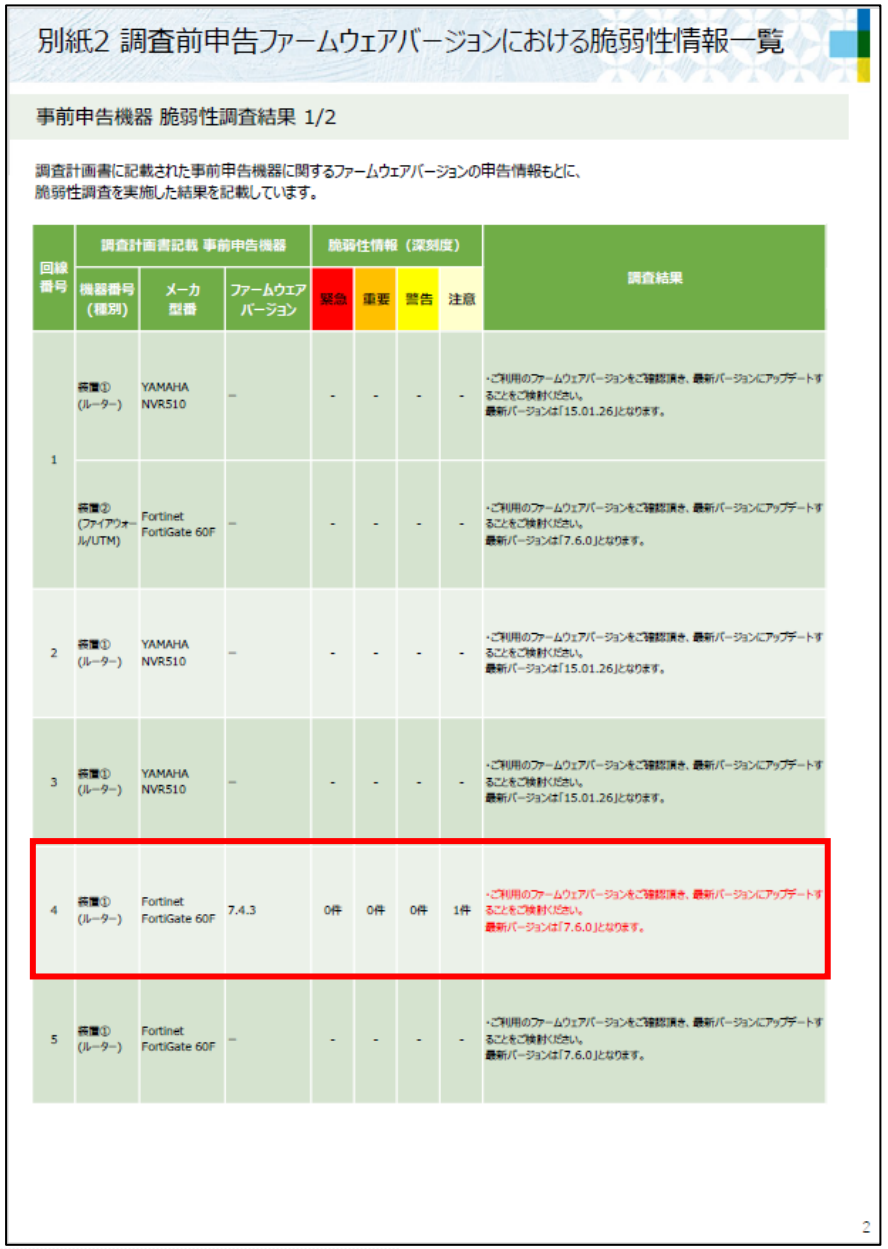
・現地で確認できた機器について、下記内容を記載しています。

・ログインによるファームウェアバージョンの確認可否
・最新のファームウェアバージョン
・ご利用中のファームウェアバージョンで確認されている脆弱性

・ログイン未実施の機器は、最新のファームウェアバージョンのみ記載しています。

別紙2【調査前申告ファームウェアバージョンにおける脆弱性情報一覧】
ご提出いただいた「医療機関記入依頼書」に基づき、事前にファームウェアバージョンをご共有いただいた機器の脆弱性情報を記載しています。

補足　別紙2【調査前申告ファームウェアバージョンにおける脆弱性情報一覧】



別紙2 調査前申告ファームウェアバージョンにおける脆弱性情報一覧

事前申告機器 脆弱性調査結果 1/2

調査計画書に記載された事前申告機器に関するファームウェアバージョンの申告情報もとに、
脆弱性調査を実施した結果を記載しています。

回線番号	調査計画書記載 事前申告機器			脆弱性情報（深刻度）				調査結果
	機器番号（種別）	メーカ型番	ファームウェアバージョン	緊急	重要	警告	注意	
1	装置①（ルーター）	YAMAHA NVR510	–	-	-	-	-	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「15.01.26」となります。
	装置②（ファイアウォール/UTM）	Fortinet FortiGate 60F	–	-	-	-	-	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「7.6.0」となります。
2	装置①（ルーター）	YAMAHA NVR510	–	-	-	-	-	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「15.01.26」となります。
3	装置①（ルーター）	YAMAHA NVR510	–	-	-	-	-	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「15.01.26」となります。
4	装置①（ルーター）	Fortinet FortiGate 60F	7.4.3	0件	0件	0件	1件	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「7.6.0」となります。
5	装置①（ルーター）	Fortinet FortiGate 60F	–	-	-	-	-	・ご利用のファームウェアバージョンをご確認頂き、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。 最新バージョンは「7.6.0」となります。

2

・「医療機関記入依頼書」にファームウェアバージョンを記載いただいた機器は、「別紙2【調査前申告ファームウェアバージョンにおける脆弱性情報一覧】」に脆弱性情報を記載しています。

・「回線番号」は「調査実施計画一覧」に紐づいています。

・「ファームウェアバージョン」欄には「医療機関記入依頼書」に記入いただいた内容を記載、「調査結果」には下記内容を記載しています。

・最新のファームウェアバージョン
・ご利用中のファームウェアバージョンに確認されている脆弱性

・脆弱性情報の詳細は、巻末の「事前申告機器 脆弱性詳細」をご確認ください。

調査実施計画一覧

医療機関名	サンプル病院

■注意事項
・装置バージョン確認は、対象装置のアカウント/パスワードの確認ができており、調査当日にログインできることを前提としています。
・脆弱性診断は、グローバルIPアドレスが判明している必要があります。特に、動的IPの場合は、調査当日確認したグローバルIPアドレスを連携いただくことを前提としています。

【凡例】
○ … 調査実施予定
× … 調査対象外
－ … 指定なし

調査実施項目

	用途、システム名	装置バージョン確認						脆弱性診断	備考
		装置①							
			メーカー	機種名					
回線1	電子カルテ	○	YAMAHA	NVR510					
回線2	医事	○	YAMAHA	NVR510					
回線3	オンライン資格システム	×	YAMAHA	NVR510					
回線4	自動精算機クレジットカード決済用	×	Fortinet	FortiGate 60F	－			×	
回線5	検査	×	Fortinet	FortiGate 60F	－			×	
回線6	放射線	×	Fortinet	FortiGate 60F	－			×	
回線7	放射線	×	YAMAHA	RTX810	－			×	

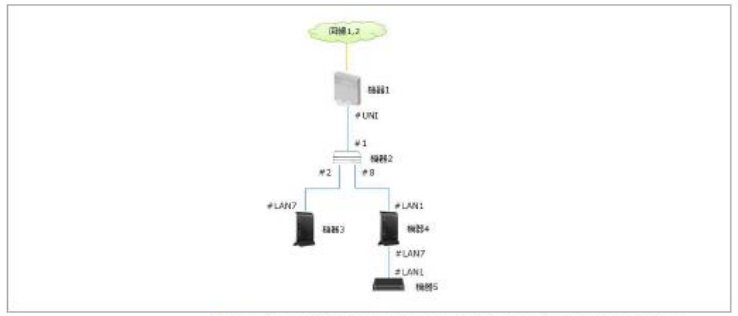
「医療機関記入依頼書」にファームウェアバージョンの記載あり

「2. 外部ネットワーク接続機器調査」について

2. 外部ネットワーク接続機器調査 1/3

現地調査機器

現地調査で確認した稼働中のファームウェアバージョン情報をもとに、脆弱性調査を実施した結果を記載しています。



※詳細は「別紙1_<連番>_<医療機関名>【現地調査報告書】_YYYYMMDD.pdf」をご参照ください。

補足④

回線番号	現地調査機器 機器番号(種別)	メーカ型番	ファームウェアバージョン	脆弱性情報(深刻度) 緊急	重要	警告	注意	調査結果
1~2	機器3 (ルータ)	YAMAHA NVR510	15.01.02	0件	3件	2件	0件	・装置にログインし、ファームウェアバージョン確認を実施しました。 ファームウェアバージョンが最新ではありませんでしたので、運用との兼ね合いを考慮し、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。最新バージョンは、「15.01.26」となります。 ・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。 貴院への影響度合の確認をお願いします。脆弱性情報の詳細は「6
	機器4 (ルータ)	YAMAHA NVR510	確認未実施 (ID-PASS不明 or相違)	-	-	-	-	・今回の調査では利用されているファームウェアバージョンを確認することができませんでした。 ご利用のファームウェアバージョンをご確認頂き、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。最新バージョンは「15.01.26」となります。
	機器5 (UTM-FW)	Fortinet FortiGate60F	7.4.3	0件	0件	3件	2件	・装置にログインし、ファームウェアバージョン確認を実施しました。 ファームウェアバージョンが最新ではありませんでしたので、運用との兼ね合いを考慮し、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。最新バージョンは、「7.6.0」となります。 ・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。 貴院への影響度合の確認をお願いします。脆弱性情報の詳細は「6.補足資料」をご確認ください。

→脆弱性情報 計5件

1

補足④

・巻頭「表記について」の「脆弱性の評価基準」に基づき、ご利用中のファームウェアバージョンに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、ネットワーク管理者にご相談ください。
・なお、緊急・警告は速やかな対処が必要な脆弱性情報です。脆弱性情報の詳細は、6章「補足資料」に記載しています。

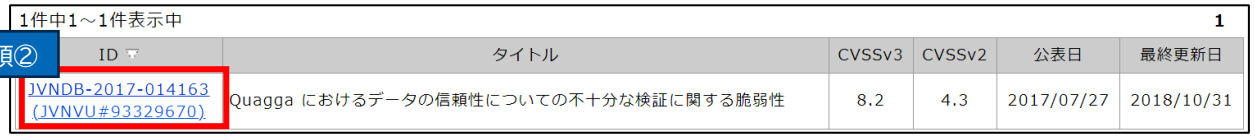
メーカ・型番	YAMAHA NVR510	ファームウェアバージョン	15.01.02
現地調査機器(機器番号)	機器3,機器4		

※

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-2020-5548	7.5	15.01.14以前	ヤマハ製の複数のネットワーク機器におけるサービス運用妨害 (DoS) の脆弱性
CVE-2016-2183	7.5	15.01.26以前	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	15.01.26以前	IKEv1 のメインモードに総当たり攻撃に対する脆弱性
CVE-2021-20844	5.7	15.01.18以前	HTTP レスポンスヘッダインジェクション
CVE-2021-20843	5.4	15.01.18以前	クロスサイトスクリプトインクルージョン

※脆弱性番号
脆弱性対策情報データベースに基づき、検出された脆弱性情報の脆弱性番号を記載しています。
脆弱性番号から脆弱性情報の詳細が確認可能です(次頁で解説)。

補足　脆弱性情報の確認方法




公開日：2017/07/28　最終更新日：2018/03/22

JVNVU#93329670
Open Shortest Path First (OSPF) プロトコルの複数の実装に Link State Advertisement (LSA) の扱いに関する問題

概要
Open Shortest Path First (OSPF) プロトコルを実装する複数の製品には、シーケンス番号が MaxSequenceNumber になっている Link State Advertisement (LSA) の扱いに問題が存

影響を受けるシステム
- OSPF プロトコルを実装している製品

詳細情報
データの整合性検証不備 (CWE-354) - CVE-2017-3224, CVE-2017-3752, CVE-2017-6770
OSPF プロトコルを実装する複数の製品には、シーケンス番号が MaxSequenceNumber となっている LSA の扱いに問題が存在します。

OSPF プロトコルでは、同一の LSA が存在する場合により新しい LSA を選択する処理が規定されています。RFC2328 セクション 13.1 では、同一の LSA を比較してどちらがより新しい LSA であるかを判別するアルゴリズムとして

1. シーケンス番号がより大きいもの
2. チェックサムの値がより大きいもの
3. age フィールドの値が一方のみ MaxAge であった場合は MaxAge のもの
4. (以下省略)

といった手順が規定されています。
また、ルーティングドメイン内のルータが保持している LSA のうち、シーケンス番号が MaxSequenceNumber となったものを廃棄させるため、age フィールドの値を MaxAge にした LSA を配布する "premature aging" という処理が規定されています。
しかし RFC2328 では、"premature aging" の際に配布する LSA と廃棄対象の LSA が持っているリンク情報が同一でなければならない、という明確な記載はありません。そのため、実装によっては、廃棄対象となる LSA が持っているリンク情報とは異なる、ルータが本来持っているリンク情報を持った LSA による premature aging が行われることがあります。
このような実装を使用しているネットワークにおいては、シーケンス番号が MaxSequenceNumber で不正なリンク情報を持ち、チェックサムの値が既存の LSA より大きくなるように細工した LSA を注入された場合、premature aging 処理によって細工された LSA の廃棄処理が試みられても、実際に配布される LSA よりも細工された LSA のチェックサム値が大きいために、細工された LSA がより新しいものであると見なされ、廃棄されない状態になってしまいます。その結果、同一ルーティングドメイン内に接続されているルータのルーティングテーブルが改ざんされる可能性があります。

CVE-2017-3224 は、本脆弱性の影響を受ける Quagga、ならびに Quagga を含んでいる SUSE, openSUSE, Red Hat packages などの Linux ディストリビューションを対象として、CVE-2017-3752 は、本脆弱性の影響を受ける Lenovo の 製品を対象として、また CVE-2017-6770 は、本脆弱性の影響を受ける Cisco の 製品 に、それぞれ付与されています。

想定される影響
細工された LSA を注入されることで、ルーティングテーブルの内容を改ざんされ、サービス運用妨害 (DoS) 攻撃を受けたり、ネットワークトラフィックを別のルータに誘導されたりする可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに、最新版にアップデートしてください。

■手順

手順① 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

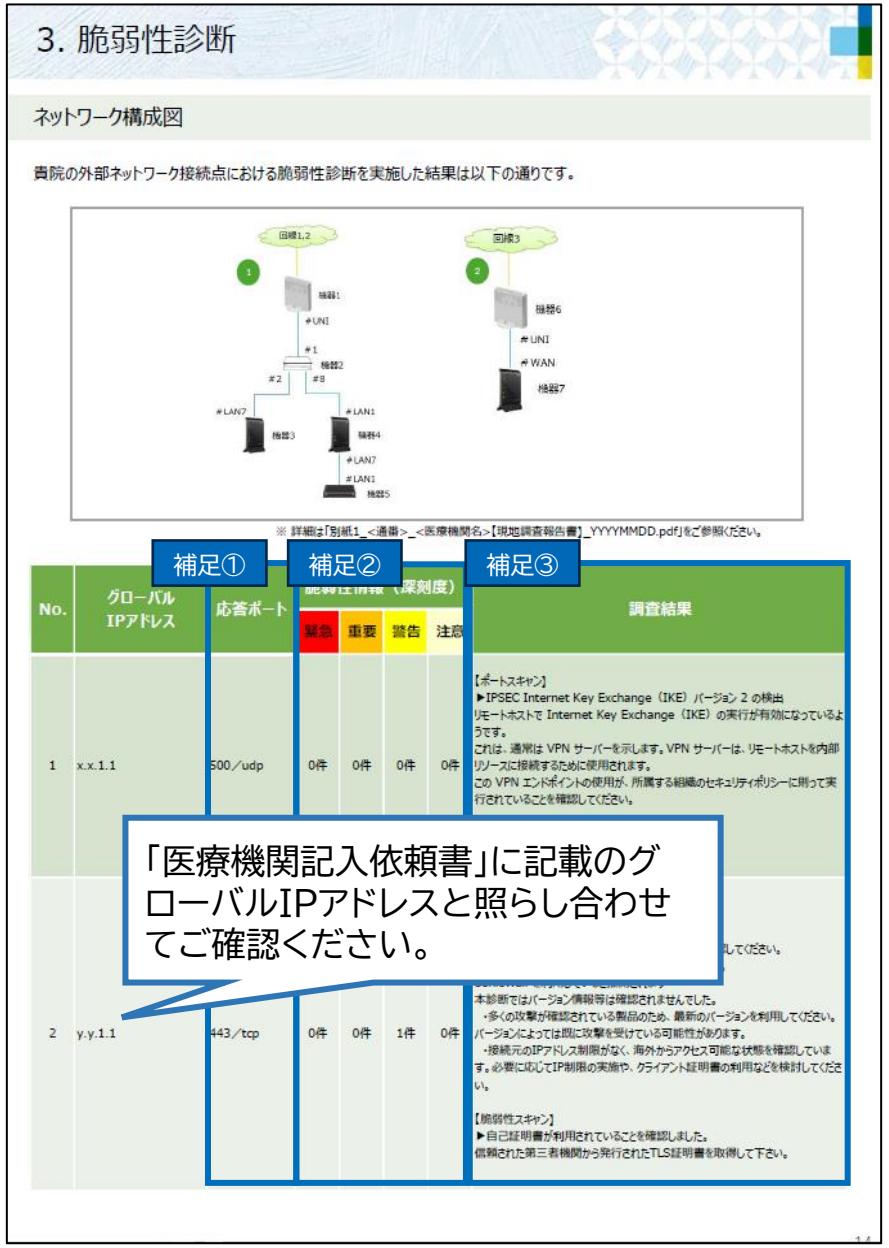
手順② ID欄のリンクを押下

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

脆弱性情報の詳細、影響、対策方法等が示されています。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。

「3. 脆弱性診断」について

「3. 脆弱性診断」について



補足①

グローバルIPアドレスごとに応答のあったポートを記載しています。

補足②

「2. 外部ネットワーク接続機器調査」と同様、検出された脆弱性情報の件数と深刻度を記載しています。

補足③

【ポートスキャン】
該当する回線のグローバルIPアドレスに対してリモートアクセスを実施しています。

空きポートが検出された場合、システム運用上、必要なポートであるかご確認ください。未使用ポートである場合は、ポートを閉じる等の対策を検討してください。

【脆弱性スキャン】
ポートスキャンで確認された空きポートに対して脆弱性を調査しています。

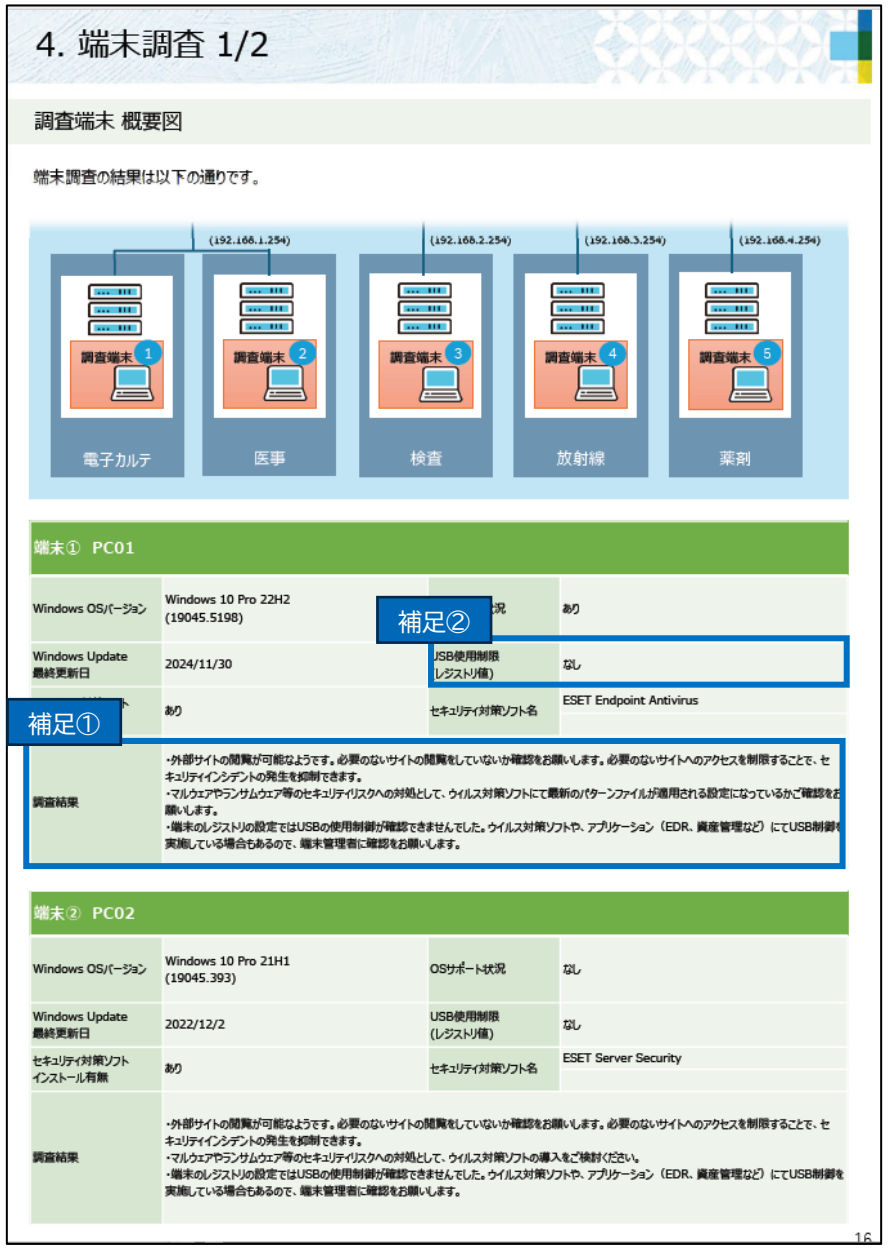
脆弱性が検出された場合は、ネットワーク管理者にご相談ください。

別紙3【脆弱性診断報告書】
本紙で通知している脆弱性情報の詳細を掲載しています。本調査で脆弱性情報が検出された場合、本紙と併せてベンダー等に提出し、対処策を検討することを推奨します。

別紙4【脆弱性診断早期報告】
脆弱性診断にて早急な対応が必要となる脆弱性が検出された場合にのみ作成されます。

「4. 端末調査」について

「4. 端末調査」について



4. 端末調査 1/2

調査端末 概要図

端末調査の結果は以下の通りです。

端末① PC01			
Windows OSバージョン	Windows 10 Pro 22H2 (19045.5198)	OSサポート状況	あり
Windows Update 最終更新日	2024/11/30	USB使用制限 (レジストリ値)	なし
セキュリティ対策ソフト インストール有無	あり	セキュリティ対策ソフト名	ESET Endpoint Antivirus
調査結果	・外部サイトの閲覧が可能なようです。必要のないサイトの閲覧をしていないか確認をお願いします。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。 ・マルウェアやランサムウェア等のセキュリティリスクへの対処として、ウイルス対策ソフトにて最新のパターンファイルが適用される設定になっているかご確認をお願いします。 ・端末のレジストリの設定ではUSBの使用制御が確認できませんでした。ウイルス対策ソフトや、アプリケーション（EDR、資産管理など）にて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 PC02			
Windows OSバージョン	Windows 10 Pro 21H1 (19045.393)	OSサポート状況	なし
Windows Update 最終更新日	2022/12/2	USB使用制限 (レジストリ値)	なし
セキュリティ対策ソフト インストール有無	あり	セキュリティ対策ソフト名	ESET Server Security
調査結果	・外部サイトの閲覧が可能なようです。必要のないサイトの閲覧をしていないか確認をお願いします。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。 ・マルウェアやランサムウェア等のセキュリティリスクへの対処として、ウイルス対策ソフトの導入をご検討ください。 ・端末のレジストリの設定ではUSBの使用制御が確認できませんでした。ウイルス対策ソフトや、アプリケーション（EDR、資産管理など）にて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。		

16

補足①

補足②

補足①

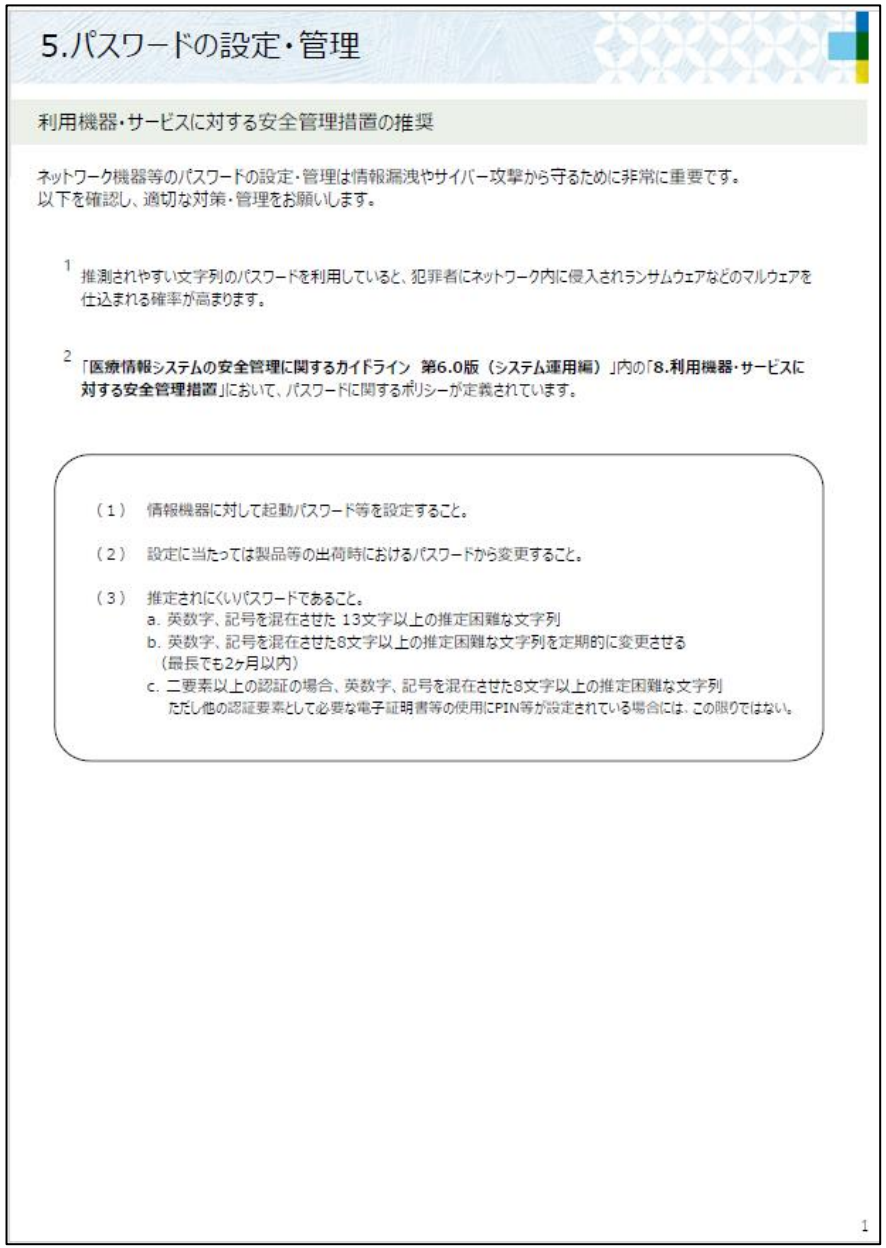
端末調査の結果を記載しています。セキュリティ対策状況をご確認いただき、対策が必要な場合は、端末管理者にご相談ください。

補足②

「USB使用制限」は、OSの設定値（レジストリ値）でUSBポートの使用制限状況を確認した結果を示しています。
調査結果が「なし」の場合であっても、アプリケーションやウイルスソフト等で制御されている場合がありますので、端末管理者にご確認ください。

「5. パスワードの設定・管理」について

「5. パスワードの設定・管理」について



5.パスワードの設定・管理

利用機器・サービスに対する安全管理措置の推奨

ネットワーク機器等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、犯罪者に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] 「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」において、パスワードに関するポリシーが定義されています。

（1） 情報機器に対して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を定期的に変更させる
（最長でも2ヶ月以内）
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。

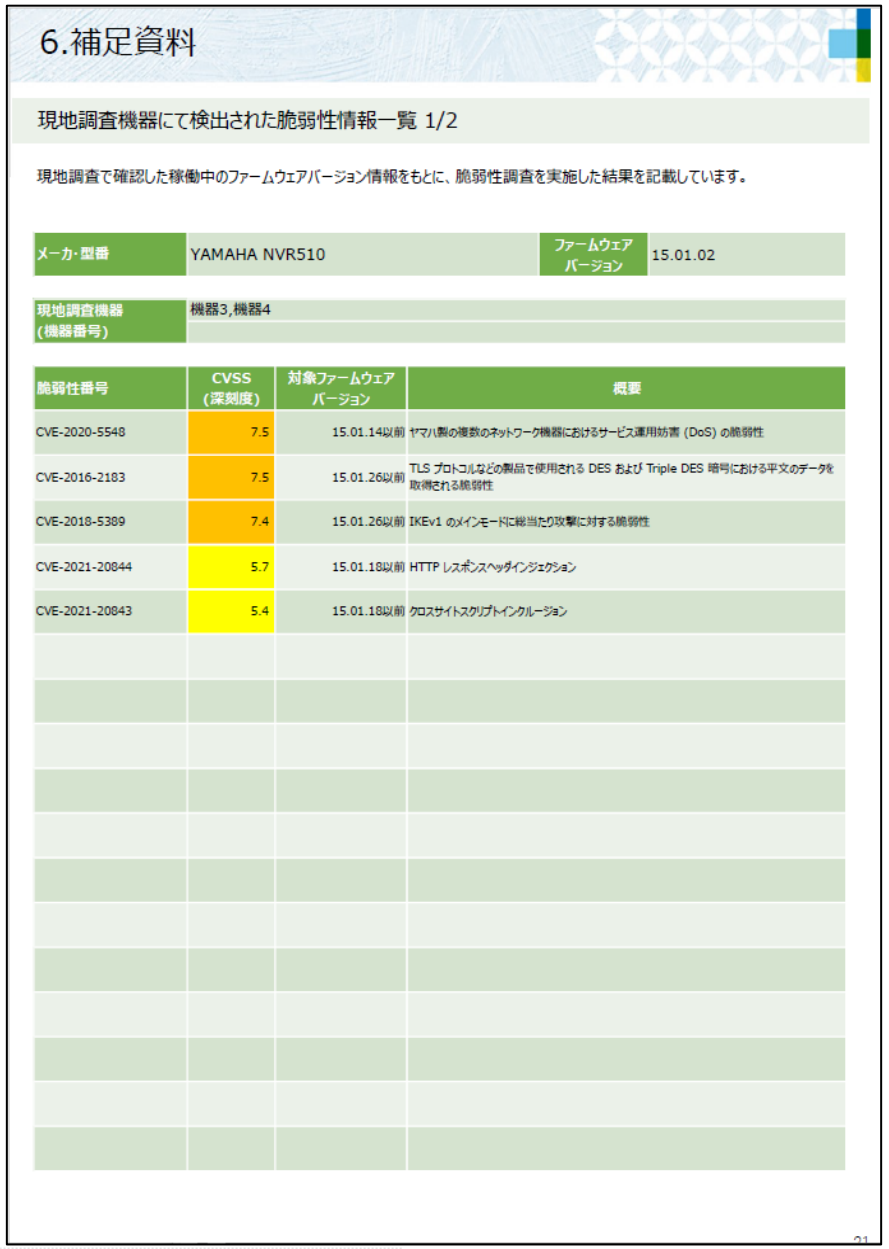
1

・ネットワーク機器におけるパスワードポリシーを記載しています。

・「医療機関記入依頼書」記入時にパスワードの設定状況をご確認いただきましたが、本章の内容をご確認いただき、現在のパスワード設定状況・管理方法の見直し、「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）」に合わせた適切なご対応をお願いします。

「6. 補足資料」について

「6. 補足資料」について



6.補足資料

現地調査機器にて検出された脆弱性情報一覧 1/2

現地調査で確認した稼働中のファームウェアバージョン情報をもとに、脆弱性調査を実施した結果を記載しています。

メーカ・型番	YAMAHA NVR510	ファームウェアバージョン	15.01.02
現地調査機器(機器番号)	機器3,機器4		

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-2020-5548	7.5	15.01.14以前	ヤマハ製の複数のネットワーク機器におけるサービス運用妨害 (DoS) の脆弱性
CVE-2016-2183	7.5	15.01.26以前	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	15.01.26以前	IKEv1 のメインモードに総当たり攻撃に対する脆弱性
CVE-2021-20844	5.7	15.01.18以前	HTTP レスポンスヘッダインジェクション
CVE-2021-20843	5.4	15.01.18以前	クロスサイトスクリプトインクルージョン

21

・「2. 外部ネットワーク接続機器調査」において、現地調査機器にて検出された脆弱性情報の詳細を一覧で記載しています。(P.17参照)

・「2. 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。

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