

令和6年度版

医療機関確認用

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

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （ 3 / 31 ）	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果			備考	R5年度 項目
		（日付）				
		1回目	目標日	2回目		
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。					
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ (3 / 31)	(7 / 31)	はい・いいえ (/)		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	アクセスログを管理している。(2-(6))	はい・いいえ (3 / 31)	(7 / 31)	はい・いいえ (/)		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		
ネットワーク機器について、以下を実施している。						
セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※	
接続元制限を実施している。(2-(8))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※	
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ (3 / 31)	(7 / 31)	はい・いいえ (/)		
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ (3 / 31)	(7 / 31)	はい・いいえ (/)		

- 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「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（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目

令和6年度

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

事業者確認用

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果 (日付)			備考	R5年度 項目
		1回目	目標日	2回目		
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
2 医療情報システム の管理・ 運用	医療情報システム全般について、以下を実施している。					
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。(2-(3))	はい・いいえ (3 / 31)	(7 / 31)	はい・いいえ (/)		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	アクセスログを管理している。(2-(6))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		
	ネットワーク機器について、以下を実施している。					
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※
接続元制限を実施している。(2-(8))	(はい)・いいえ (3 / 31)	(/)	はい・いいえ (/)		※	

事業者名： _____

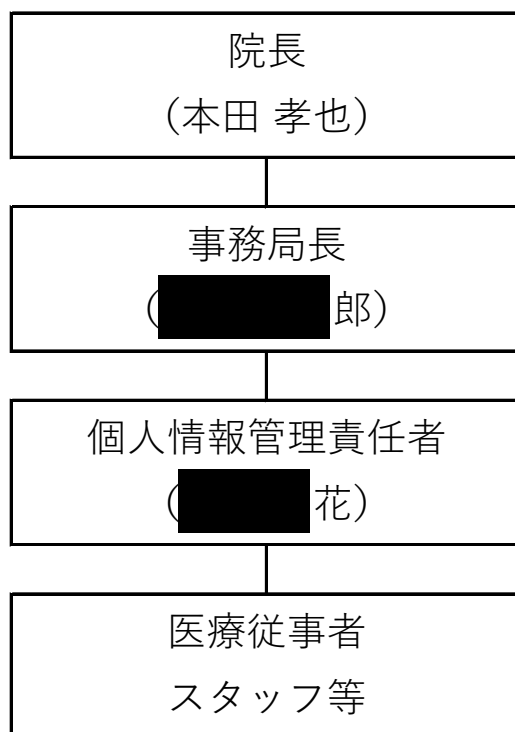
- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「医療機関におけるサイバーセキュリティ対策チェックリスト（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目

1-(1) 個人情報保護体制図

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マニュアル p.5

1 体制構築

(1) 医療情報システム安全管理責任者を設置している。



2-(1) ソフト一覧

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マニュアル p.6

2 医療情報システムの管理・運用

(1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)

ソフト	version	事業者	連絡先	備考
WebORCA	最新	日本医師会	weborca-support @orcamo.jp	レセコン
NIM	2.1.0	NIM	095-838-2066	電子カルテ
OqsComApp	最新	社会保険診療報酬支払 基金情報化企画部 情報化支援部	0800-0804583	顔認証付きカードリー ダー連携アプリケー ション
OqsDistroApp	最新	社会保険診療報酬支払 基金情報化企画部 情報化支援部	0800-0804583	顔認証付きカードリー ダー配信アプリケー ション
レセプトチェッカー	最新	NIM	095-838-2066	レセプトチェックソフト
FCR PRIMA T2 本体ソフトウェア		富士フイルム	095-837-8273	レントゲン

2-(1)(2) 機器一覧

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マニュアル p.6～7

2 医療情報システムの管理・運用

- (1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)
- (2) リモートメンテナンス(保守)を利用している機器の有無を事業者を確認した。(医療情報システム全般)

メーカー	OS・製品名	ソフト	コンピューター名	場所	IP ADDRESS	リモートメンテ
DELL	Windows11 Home 22H2	あじさいネット	DESKTOP- QJM38Q70	診察室	動的 あじさいネット: 172.31.255.1	無
eMachines	Windows 7 Home Premium	NIM WebORCA	honda-PC	診察室	動的	無
HP	Windows10 Pro 1511		CV672332650	レントゲン室	動的	無
HP	Windows 11 Home	レセ電ビュー ワー2.5.0 ORCAMO クラ イアント monsiaj 2.0.31 オンライン請 求システム・ 長崎県	DESKTOP- UGDPDR4	受付	動的	無
EPSON	Windows 10 Home		DESKTOP- Q5SP4M5	受付	IP: 手動 (固定) 192.168.1.211	無
I-O DATA	Windows 10EnteroricEL TSC 1809	WebORCA	R-ONSI-PC	受付	172.31.10.10 169.254.30.188/ 16	無
DELL	Windows 10 Pro 22H2		DESKTOP- 50T943L	院長室	動的	無
PFU	Caora PD- CA01			受付		無
富士 ファイルム	FCR PRIMA T2	本体ソフト		診察室		無

2-(1)(4)(5) 利用者一覧

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マニュアル p.6～8

2 医療情報システムの管理・運用

- (1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)
- (4) 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(サーバ、端末 PC)
- (5) 退職者や使用していないアカウント等、不要なアカウントを削除している。(サーバ、端末 PC)

ソフト	ID	利用者	権限	備考
WebORCA	master	院長・事務	管理者	レセコン
NIM	admin	院長	管理者	電子カルテ
OqsComApp	admin	院長・事務	管理者	顔認証付きカードリーダー連携アプリケーション
OqsDistroApp	admin	院長・事務	管理者	顔認証付きカードリーダー配信アプリケーション
レセプトチェッカー	admin	院長	管理者	レセプトチェックソフト
FCR PRIMA T2 本体ソフトウェア	admin	院長	管理者	レントゲン

2-(3) セキュリティ開示書請求

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マニュアル p.7

2 医療情報システムの管理・運用

(3) 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらう。(医療情報システム全般)

ソフト及び機器	事業者	連絡先	備考
WebORCA	日本医師会	weborca-support@orcamo.jp	レセコン
NIM	NIM	095-838-2066	電子カルテ
レセプトチェッカー	NIM	095-838-2066	レセプトチェックソフト
FCR PRIMA T2	富士フイルム	095-837-8273	レントゲン

2-(6) ログ管理

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マニュアル p.9

2 医療情報システムの管理・運用

(6) アクセスログを管理している。(サーバ)

ソフト及び機器	場所	コンピューター名	備考
WebORCA	診察室	honda-PC	レセコン
WebORCA	受付	DESKTOP-UGPDPR4	レセコン
NIM	診察室	honda-PC	電子カルテ
レセプトチェッカー	診察室	honda-PC	レセプトチェック ソフト

2-(7) ネットワーク関連診断内容

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マニュアル p.10

2 医療情報システムの管理・運用

(7) セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

診断結果

接続元IPドレス	OS	時刻
133.218.30.220	macOS	2023年10月11日 15時40分13秒

ランサムウェア 「Wannacry/ GoldenEye」 (tcp/445)	SSH (22/tcp)	TELNET (23/tcp)	NETBIOS (139/tcp)
✓ 安全な設定です	✓ 安全な設定です	✓ 安全な設定です	✓ 安全な設定です
RDP (3389/tcp)	VNC (5900/tcp)		
✓ 安全な設定です	✓ 安全な設定です		

2-(7) ルーターファームウェア画面

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マニュアル p.10

2 医療情報システムの管理・運用

(7) セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

The screenshot displays the Buffalo router's web management interface. The top navigation bar includes the Buffalo logo and icons for home, global settings, information, download, and share. A sidebar on the left lists various settings categories: Internet, LAN, 無線設定 (Wireless Settings), セキュリティ (Security), アプリケーション (Applications), 管理 (Management), システム設定 (System Settings), ログ (Logs), 設定管理/再起動 (Settings Management/Restart), ファームウェア更新 (Firmware Update), and ステータス (Status). The main content area is titled 'ファームウェア更新' (Firmware Update) and shows the current version as 'WSR-2533DHPL Ver.1.09'. The update method is set to 'ローカルファイル指定' (Local File Specified). A 'ファイル名' (File Name) field is empty, with a message 'ファイルを選択 選択されていません' (Select a file, none selected). A '更新実行' (Execute Update) button is present. Below this, a note states '※ファームウェアは、下のリンクからダウンロードできます。' (Firmware can be downloaded from the link below) with a link to 'ファームウェアダウンロードサイト' (Firmware Download Site). The '拡張設定' (Advanced Settings) section includes 'ファームウェア自動更新機能' (Firmware Auto Update Function) set to '重要な更新のみ行う' (Perform only important updates), '現在時刻' (Current Time) as '2023年 10月 11日 (水曜日) 15:14' with a '現在の状態を表示する' (Show current status) button, and '更新時刻' (Update Time) set to '毎日 4:00 - 4:59'. A '設定' (Settings) button is at the bottom.

2-(8) ルーター接続制限画面

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マニュアル p.11

2 医療情報システムの管理・運用

(8) 接続元制限を実施している。(ネットワーク)

The screenshot shows the configuration page for a Buffalo AirStation WXR-5950AX12 router. The page is titled "システム設定" (System Settings) and includes a sidebar with options like "ログ" (Log), "設定管理/再起動" (Configuration Management/Restart), "ファームウェア更新" (Firmware Update), and "ステータス" (Status). The main content area is divided into several sections:

- アクセス (Access):** A table with columns for "有効" (Enabled), "制限項目" (Restriction Item), and "パケット数" (Packet Count).

有効	制限項目	パケット数
<input checked="" type="checkbox"/>	無線LANからの設定を禁止する	0
<input type="checkbox"/>	有線LANからの設定を禁止する	0
- Internet側リモートアクセス設定 (Internet Side Remote Access Settings):** A section with a "有効" (Enabled) checkbox and a "制限項目" (Restriction Item) "Internet側リモートアクセス設定を許可する" (Allow Internet Side Remote Access Settings).
- デバイスコントロール (Device Control):** A section with a "有効" (Enabled) checkbox and a "制限項目" (Restriction Item) "デバイスに対しポートスキャンを実行する" (Execute Port Scan on Device).
- 時刻 (Time):** A section for NTP settings. It includes a "NTP機能" (NTP Function) checkbox checked "使用する" (Use), a "サーバー名" (Server Name) field with "ntp.jst.mfeed.ad.jp", a "確認時間" (Check Interval) field with "24" and "時間毎" (Every Hour), and a date/time picker showing "2020年3月24日" (March 24, 2020) at "7時28分36秒" (7:28:36 AM) in the "(GMT+09:00)東京、大阪、ソウル" (GMT+09:00) Tokyo, Osaka, Seoul time zone. There are buttons for "現在の時刻を表示" (Show Current Time) and "現在アクセス中のパソコンから時刻を取得" (Get Time from Currently Accessing PC).

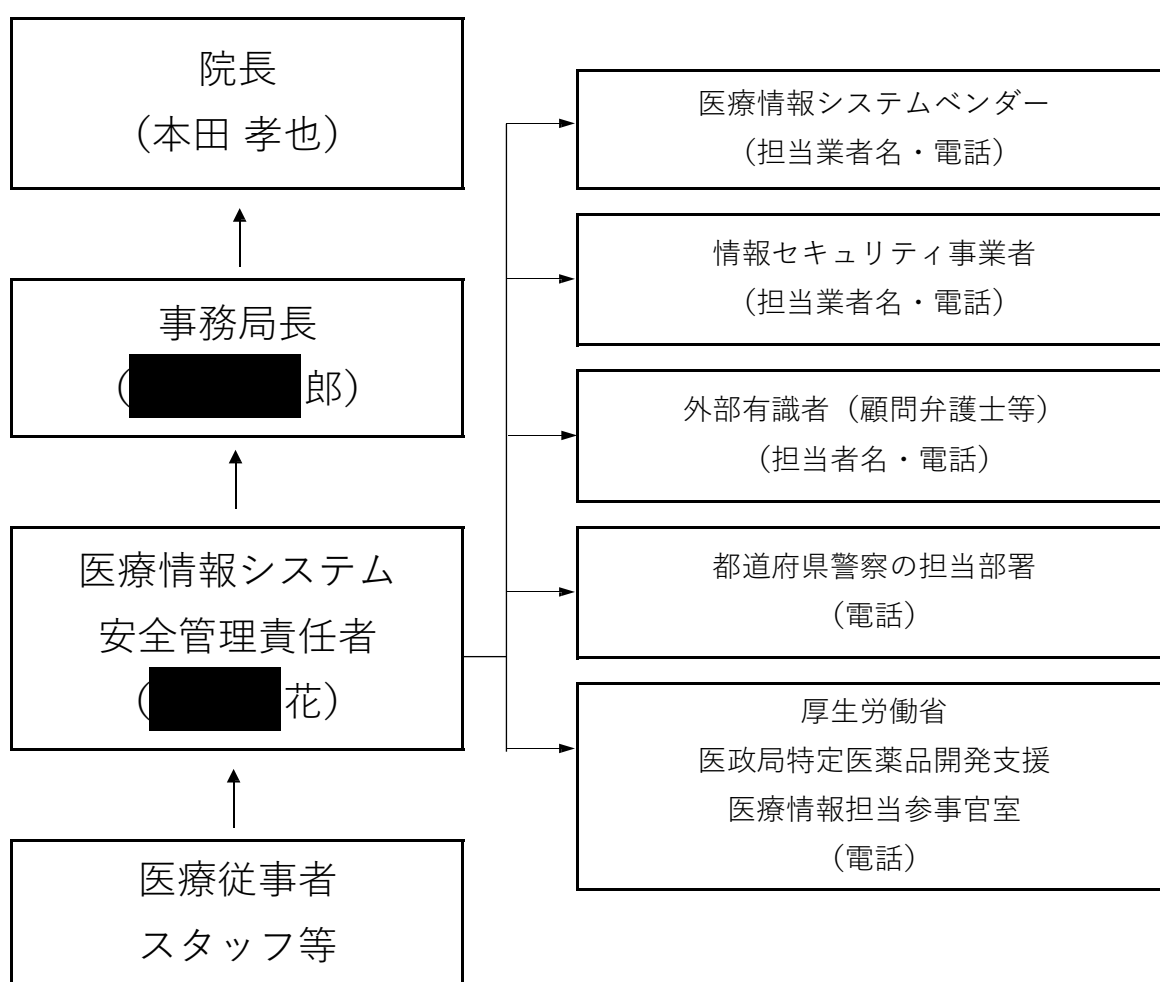
The footer of the page displays "AirStation WXR-5950AX12 Version 3.03" and "Copyright © 2019 Buffalo Inc." A "設定" (Settings) button is located at the bottom right of the configuration area.

3-(1) インシデント発生時における連絡体制図

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マニュアル p.12

3 インシデント発生に備えた対応

(1) インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。



その他

医療情報システムの管理・運用で補助的に必要な要素です。チェック内容とは異なります。

ウイルス対策ソフトウェア			
ソフト及び機器	場所	コンピューター名	備考
F-secure	診察室	DESKTOP-QJM38Q70	あじさいネット
Windows Defender Windows ファイア ウォール	診察室	honda-PC	NIM WebORCA
Windows Defender	受付	DESKTOP-UGPDPR4	レセ電ビューワー (jma-receview) 2.5.0 WebORCA ORCAMO クライアン ト monsiaj 2.0.31 オンライン請求システ ム・長崎県
Windows Defender	受付	DESKTOP-Q5SP4M5	
Windows Defender	レントゲン室	CV672332650	

個人情報のバックアップ

個別PCでのバックアップなし：PC別ユーザーアカウントを利用しNASで対応
レントゲン室PC：外付けUSBドライブ

UTMの設置

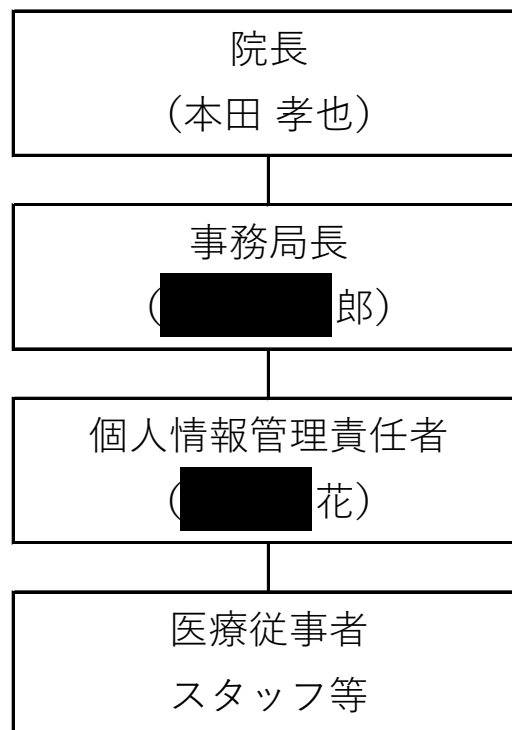
なし

1-(1) 個人情報保護体制図

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マニュアル p.5

1 体制構築

(1) 医療情報システム安全管理責任者を設置している。



2-(1) ソフト一覧

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マニュアル p.6

2 医療情報システムの管理・運用

(1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)

ソフト	version	事業者	連絡先	備考
WebORCA	最新	日本医師会	weborca-support@orcamo.jp	レセコン
NIM	2.1.0	NIM	095-838-2066	電子カルテ
OqsComApp	最新	社会保険診療報酬支払 基金情報化企画部 情報化支援部	0800-0804583	顔認証付きカードリー ダー連携アプリケー ション
OqsDistroApp	最新	社会保険診療報酬支払 基金情報化企画部 情報化支援部	0800-0804583	顔認証付きカードリー ダー配信アプリケー ション
レセプトチェッカー	最新	NIM	095-838-2066	レセプトチェックソフト
FCR PRIMA T2 本体ソフトウェア		富士フイルム	095-837-8273	レントゲン

2-(1)(2) 機器一覧

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マニュアル p.6～7

2 医療情報システムの管理・運用

- (1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)
- (2) リモートメンテナンス(保守)を利用している機器の有無を事業者を確認した。(医療情報システム全般)

メーカー	OS・製品名	ソフト	コンピューター名	場所	IP ADDRESS	リモートメンテ
DELL	Windows11 Home 22H2	あじさいネット	DESKTOP- QJM38Q70	診察室	動的 あじさいネット: 172.31.255.1	無
eMachines	Windows 7 Home Premium	NIM WebORCA	honda-PC	診察室	動的	無
HP	Windows10 Pro 1511		CV672332650	レントゲン室	動的	無
HP	Windows 11 Home	レセ電ビュー ワー2.5.0 ORCAMO クラ イアント monsiaj 2.0.31 オンライン請 求システム・ 長崎県	DESKTOP- UGDPDR4	受付	動的	無
EPSON	Windows 10 Home		DESKTOP- Q5SP4M5	受付	IP: 手動 (固定) 192.168.1.211	無
I-O DATA	Windows 10EnteroricEL TSC 1809	WebORCA	R-ONSI-PC	受付	172.31.10.10 169.254.30.188/ 16	無
DELL	Windows 10 Pro 22H2		DESKTOP- 50T943L	院長室	動的	無
PFU	Caora PD- CA01			受付		無
富士 ファイルム	FCR PRIMA T2	本体ソフト		診察室		無

2-(1)(4)(5) 利用者一覧

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マニュアル p.6～8

2 医療情報システムの管理・運用

(1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。(医療情報システム全般)

(4) 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(サーバ、端末 PC)

(5) 退職者や使用していないアカウント等、不要なアカウントを削除している。(サーバ、端末 PC)

ソフト	ID	利用者	権限	備考
WebORCA	master	院長・事務	管理者	レセコン
NIM	admin	院長	管理者	電子カルテ
OqsComApp	admin	院長・事務	管理者	顔認証付きカードリーダー連携アプリケーション
OqsDistroApp	admin	院長・事務	管理者	顔認証付きカードリーダー配信アプリケーション
レセプトチェッカー	admin	院長	管理者	レセプトチェックソフト
FCR PRIMA T2 本体ソフトウェア	admin	院長	管理者	レントゲン

2-(3) セキュリティ開示書請求

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マニュアル p.7

2 医療情報システムの管理・運用

(3) 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらう。(医療情報システム全般)

ソフト及び機器	事業者	連絡先	備考
WebORCA	日本医師会	weborca-support@orcamo.jp	レセコン
NIM	NIM	095-838-2066	電子カルテ
レセプトチェッカー	NIM	095-838-2066	レセプトチェックソフト
FCR PRIMA T2	富士フイルム	095-837-8273	レントゲン

2-(7) ネットワーク関連診断内容

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マニュアル p.10

2 医療情報システムの管理・運用

(7) セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

診断結果

接続元IPドレス	OS	時刻
133.218.30.220	macOS	2023年10月11日 15時40分13秒

ランサムウェア 「Wannacry/ GoldenEye」 (tcp/445)	SSH (22/tcp)	TELNET (23/tcp)	NETBIOS (139/tcp)
✓ 安全な設定です	✓ 安全な設定です	✓ 安全な設定です	✓ 安全な設定です
RDP (3389/tcp)	VNC (5900/tcp)		
✓ 安全な設定です	✓ 安全な設定です		

2-(7) ルーターファームウェア画面

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マニュアル p.10

2 医療情報システムの管理・運用

(7) セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

The screenshot shows the Buffalo router's web management interface. The top navigation bar includes the Buffalo logo and icons for home, global settings, information, download, and share. A sidebar on the left lists various settings categories: Internet, LAN, 無線設定 (Wireless Settings), セキュリティ (Security), アプリケーション (Applications), 管理 (Management), システム設定 (System Settings), ログ (Logs), 設定管理/再起動 (Settings Management/Restart), ファームウェア更新 (Firmware Update), and ステータス (Status). The main content area is titled 'ファームウェア更新' (Firmware Update) and displays the following information:

ファームウェアバージョン	WSR-2533DHPL Ver.1.09
更新方法	<input checked="" type="radio"/> ローカルファイル指定 <input type="radio"/> オンラインバージョンアップ
ファームウェアファイル名	ファイルを選択 <input type="text" value="選択されていません"/>

更新実行

※ファームウェアは、下のリンクからダウンロードできます。
[ファームウェアダウンロードサイト](#)

[拡張設定]

ファームウェア自動更新機能	重要な更新のみ行う
現在時刻	2023年 10月 11日 (水曜日) 15:14 <input type="button" value="現在の状態を表示する"/>
更新時刻	毎日 4:00 - 4:59

2-(8) ルーター接続制限画面

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マニュアル p.11

2 医療情報システムの管理・運用

(8) 接続元制限を実施している。(ネットワーク)

The screenshot shows the configuration page for a Buffalo AirStation WXR-5950AX12 router. The page is titled "システム設定" (System Settings) and includes a sidebar with options like "ログ" (Log), "設定管理/再起動" (Configuration Management/Restart), "ファームウェア更新" (Firmware Update), and "ステータス" (Status). The main content area is divided into several sections:

- アクセス (Access):** A table with columns for "有効" (Enabled), "制限項目" (Restriction Item), and "パケット数" (Packet Count).

有効	制限項目	パケット数
<input checked="" type="checkbox"/>	無線LANからの設定を禁止する	0
<input type="checkbox"/>	有線LANからの設定を禁止する	0
- Internet側リモートアクセス設定 (Internet Side Remote Access Settings):** A section with a "有効" (Enabled) checkbox and a "制限項目" (Restriction Item) "Internet側リモートアクセス設定を許可する" (Allow Internet Side Remote Access Settings).
- デバイスコントロール (Device Control):** A section with a "有効" (Enabled) checkbox and a "制限項目" (Restriction Item) "デバイスに対しポートスキャンを実行する" (Execute Port Scan on Device).
- 時刻 (Time):** A section for NTP settings. It includes a "NTP機能" (NTP Function) checkbox checked "使用する" (Use), a "サーバー名" (Server Name) field with "ntp.jst.mfeed.ad.jp", a "確認時間" (Check Interval) field with "24" and "時間毎" (Every Hour), and a date/time picker showing "2020年3月24日" (March 24, 2020) at "7時28分36秒" (7:28:36 AM) in the "(GMT+09:00)東京、大阪、ソウル" (GMT+09:00) Tokyo, Osaka, Seoul time zone. There are buttons for "現在の時刻を表示" (Show Current Time) and "現在アクセス中のパソコンから時刻を取得" (Get Time from Currently Accessing PC).

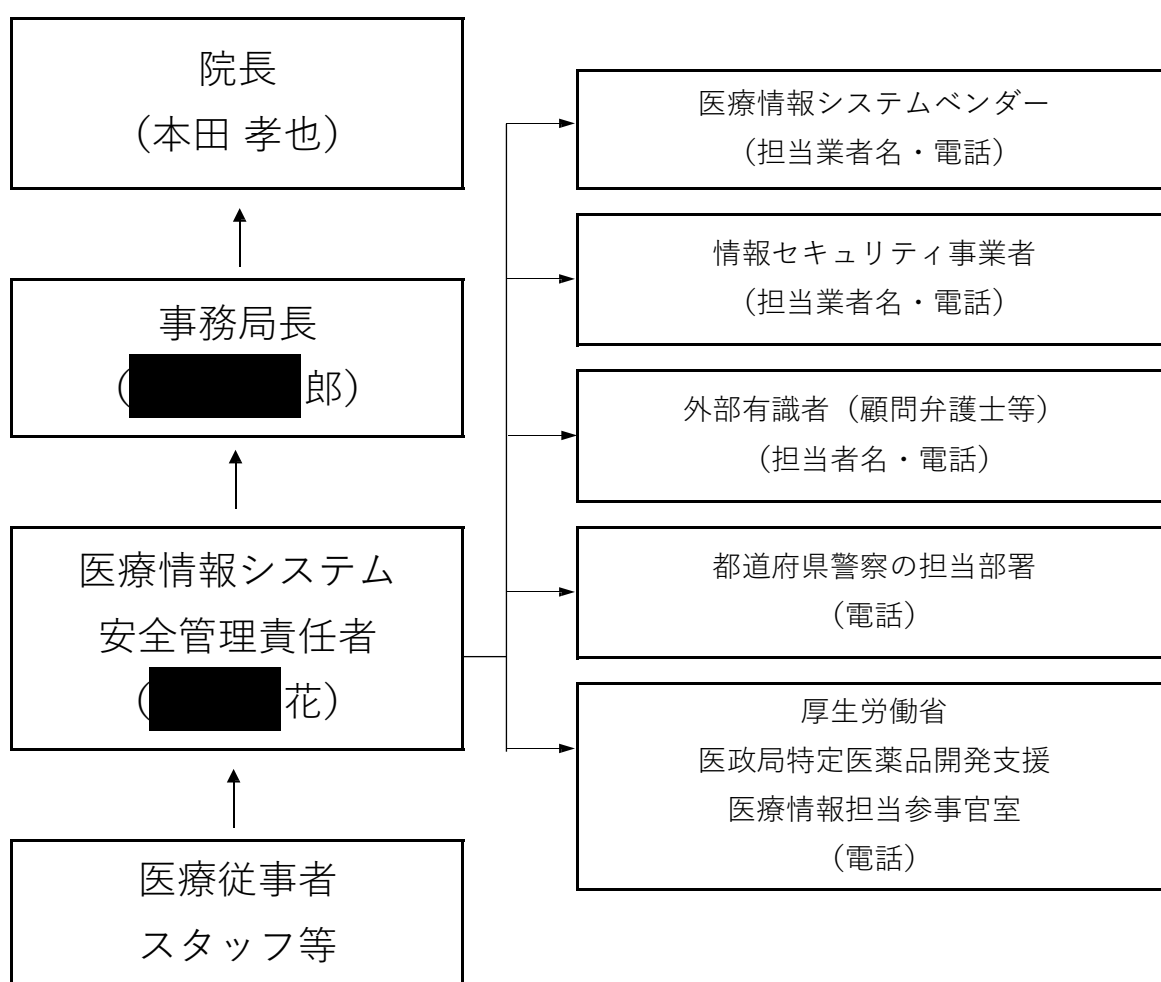
The footer of the page displays "AirStation WXR-5950AX12 Version 3.03" and "Copyright © 2019 Buffalo Inc." A "設定" (Settings) button is located at the bottom right of the configuration area.

3-(1) インシデント発生時における連絡体制図

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マニュアル p.12

3 インシデント発生に備えた対応

(1) インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。



その他

医療情報システムの管理・運用で補助的に必要な要素です。チェック内容とは異なります。

ウイルス対策ソフトウェア			
ソフト及び機器	場所	コンピューター名	備考
F-secure	診察室	DESKTOP-QJM38Q70	あじさいネット
Windows Defender Windows ファイア ウォール	診察室	honda-PC	NIM WebORCA
Windows Defender	受付	DESKTOP-UGPDPR4	レセ電ビューワー (jma-receview) 2.5.0 WebORCA ORCAMO クライアン ト monsiaj 2.0.31 オンライン請求システ ム・長崎県
Windows Defender	受付	DESKTOP-Q5SP4M5	
Windows Defender	レントゲン室	CV672332650	

個人情報のバックアップ

個別PCでのバックアップなし：PC別ユーザーアカウントを利用しNASで対応
レントゲン室PC：外付けUSBドライブ

UTMの設置

なし