セキュリティ強化ガイドライン

Imaging new visions.
ASAHIROENTGEN

改定履歴

日付	内容
2024/2/13	初版
2024/3/28	Rev.1

本書は厚生労働省発行の「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」を参考にしています。

1. セキュアな運用の指針

1) 医療情報及び情報機器を持出す必要がある場合、医療機関のシステム管理者に許諾を得ること。(7-1)

2) 保守業務を行う場合、個人情報を含むデータの持出す必要がある場合、医療機関のシステム管理者の許諾を得ること。(7-2)

3) 医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。(7-3)

4) 持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。(7-4)

5) 医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成すること。(7-7)

6) 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限すること。(7-12)

7) システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。(8-1)

8) 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。(8-2)

9) 不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。(8-3)

10) サーバのアカウントにはパスワード等を設定すること。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し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用

方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。(8-5)

11) BYOD であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。(8-9)

12) 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去すること。(10-1)

13) 保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用すること。(10-3)

14) リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。(10-5)

15) 医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能･構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。(12-1)

16) 医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。(12-2)

17) 個人情報が保管されている情報機器等の重要な情報機器には盗難防止を講じること。(12-3)

18) 記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。(12-5)

19) 医療情報システムにおいて無線 LAN を利用する場合、ANY 接続拒否、通信の暗号化等の不正利用防止策を実施すること。(13-13)

20) 医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。(18-1)

－ 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための

外部ネットワークの一時切断

- 他の情報機器への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離
- 他の情報機器への波及の調査等被害の確認のための業務システムの停止
- バックアップからの重要なファイルの復元

2. アカウント管理の指針

1) 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。(14-2)

2) 類推されやすいパスワードを使用しないこと。(14-6)

3) ID について定期的に棚卸を行い、不要なものは適宜削除すること。(14-7)

3. セキュアな使用停止の指針

1) 医療機関のネットワークからサーバを隔離すること。(E.3 a)

2) システムに保存されている患者データ及び設定データを削除すること。(E.3. b)

3) システムに保存されているデータの転送、移行、アーカイブ、削除を行うこと。(E.3 c)

4) 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。(7-10)(E.3 d)

4. 補完的リスクコントロールに関する考慮事項

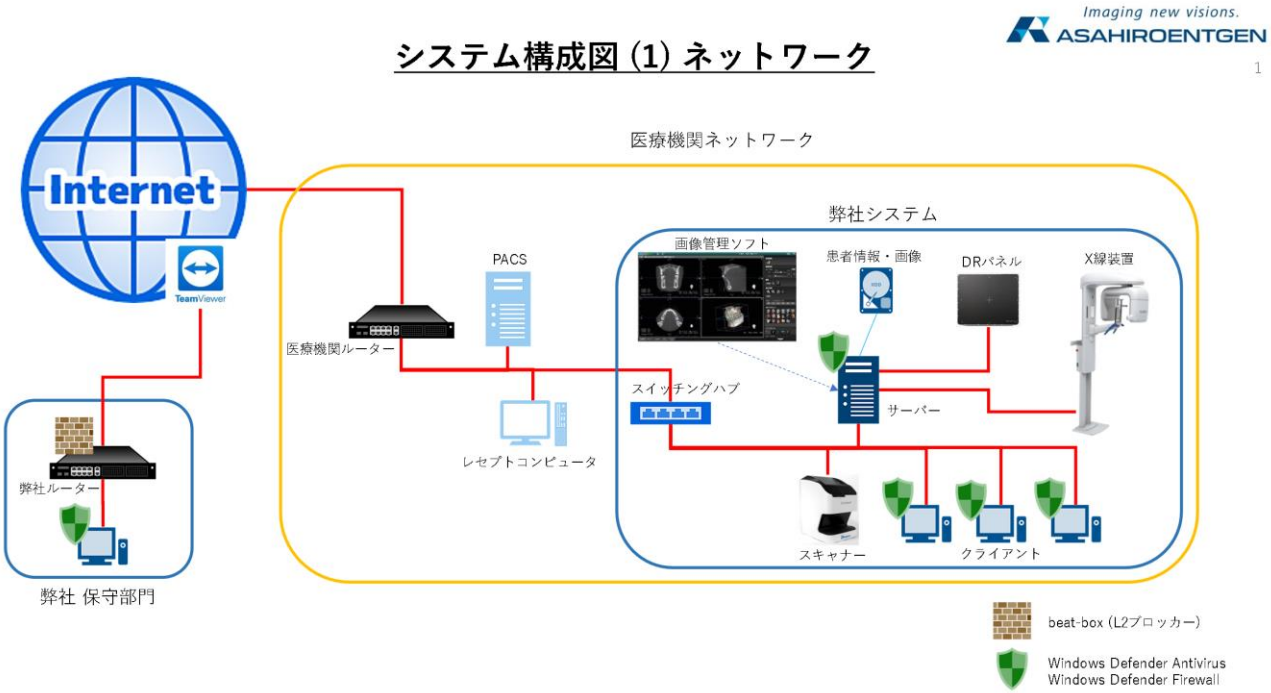
コントロールのタイプごとの補完的対策の例は下記の通りです。ご利用の環境のリスクに応じてこれらを追加で実施してください。

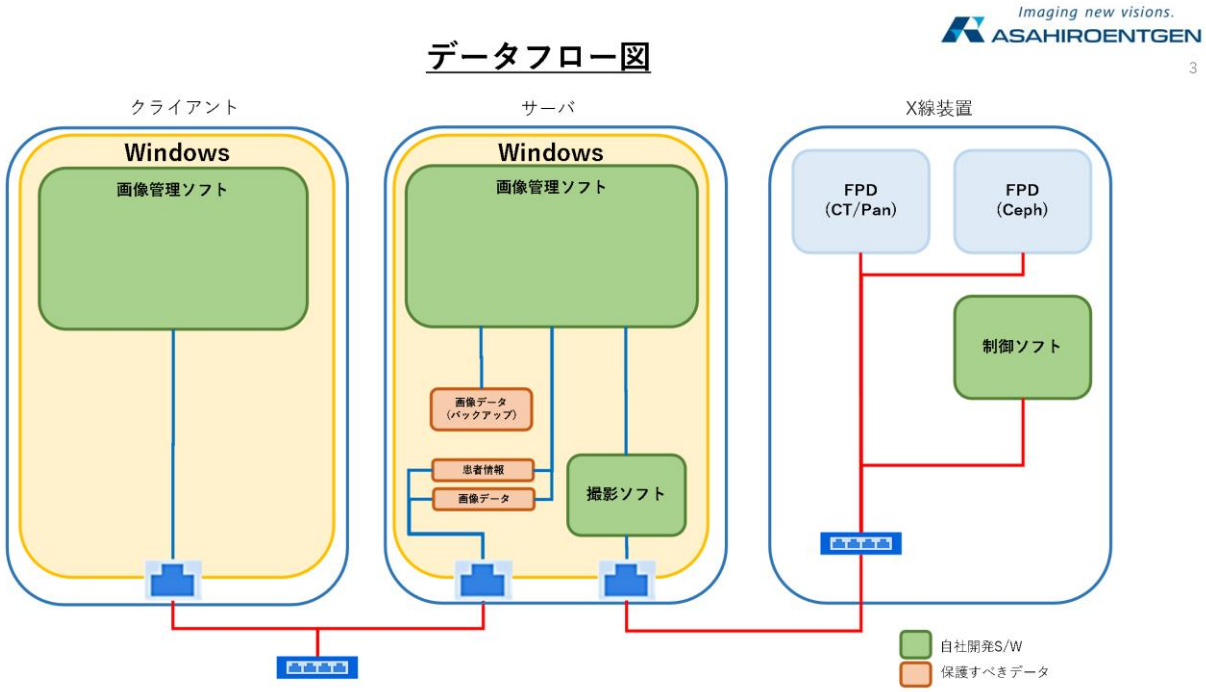
注意	**サポート終了した製品を継続して使用する場合、これらを組み合わせて実施してリスクが受容可能になるようリスクコントロールを行ってください。**

コントロールのタイプ	補完的リスクコントロール手段の例
物理的アクセスの制限	機器を物理的に制限された領域に置いて、物理的な入室管理を適切に行うことによって、機器への物理的アクセスを許可した要員だけに制限する。
リムーバブルメディアの管理	USBドライブ等のリムーバブルメディアの使用に関しては、システムのBIOS/UEFIポリシーによって、OSのポリシー又は物理的手段を通して制限する。
ネットワークの隔離	機器をネットワークから隔離する。
ネットワークの分離	機器のVLAN（仮想LAN）並びに機器が通信するその他のインフラストラクチャー及びサービスをセットアップする。
監視	侵入検知システム（IDS）、侵入予防システム（IPS）又はセキュリティ情報及び事象マネジメント（SIEM）を用いて、機器及びネットワークの疑わしい活動を監視する。
リモートアクセスの制限	機器からリモートアクセス機能を削除する。
ファイアウォール	機器を物理的又は仮想的なファイアウォールの背後に配置し、厳密に必要なネットワーク通信の特定ポートのみをファイアウォールで開放する。
マルウェア対策	機器にマルウェア対策ソフトウェアをインストールする。ネットワークから隔離された機器（スタンドアローン）については、定義の更新を必要としないソフトウェア、例えば、AIを用いたマルウェア対策ソフトウェアを用いる。
バックアップ及び復元	災害時、サイバー攻撃等によるデータ損失に対して保護及び早期復旧のために、バックアップ及び復元の手順を実装する。

5. セキュリティに関する情報共有

1)　当社システムの構成





2) 当社システムのセキュリティ対策の内容

製造業者による医療機器セキュリティ開示書、サイバーセキュリティ対策チェックリスト(事業者用)を参照ください。

3) ソフトウェア部品表

各製品の SBOM を参照ください。

4) データを送受信するネットワークポート

当社画像管理ソフトウェアでは下記のネットワークポートを使用しています。

着信ポート番号	用途
5432	データベース接続用
104（変更可）	DICOM QR 接続用
1025	当社モダリティ接続用
80, 808, 8080	画像閲覧ツールでのアクセス用（オプション）

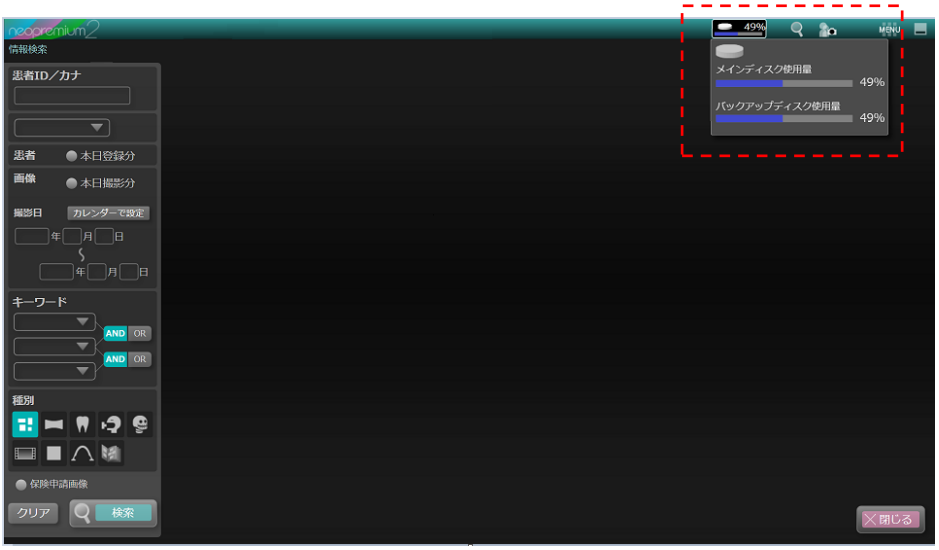
送信ポート番号	用途
7, 69, 1024	当社モダリティ接続用

5) 記録媒体及び記録機器の保管及び取扱

当社システムは患者情報、画像データをサーバ内のHDD/SSDに保存します。
これら記録媒体の保証期間はサーバの保証期間と同じです。
サーバの使用環境についてはメーカーの提示する環境仕様に準拠してください。
(温度、湿度、高度、衝撃、振動等)

6)　データの保存

当社システムは患者情報、画像データをサーバ内のストレージに保管します。
納入時のご要望に合わせた容量になっております。画像管理ソフトウェアの画面上で空き容量の目安をご確認頂けます。



データ保存量の確認画面

画像管理ソフトウェアは作成したデータをメインディスクに保管します。
システムのシャットダウン実行時にメインディスクのデータをバックアップディスクに差分コピーします。

空き容量、サーバの保証期間を踏まえて不要なデータの削除や別の記録媒体への移行、容量の大きい機器への更新等実施してください。

標準では下記のような構成になっています。

メインディスク
　D:¥MainImage　　// 撮影画像保管場所
　D:¥BackupImage　　// 撮影画像保管場所（画像のバックアップ）
　D:¥RawImage　　// 撮影画像保管場所（再構成処理前の画像データ）

バックアップディスク
　E:¥MainImage　　// 撮影画像保管場所（復旧用）
　E:¥BackupImage　　// 撮影画像保管場所（復旧用）
　E:¥RawImage　　// 撮影画像保管場所（復旧用）

システムディスク
　C:¥NEOPREMIUM2¥log　　// システムログ
　C:¥Program Files¥PostgreSQL¥***¥data// ユーザ情報、患者情報データベース（***はバージョン）

ご要望に応じてリムーバルブルメディア、ネットワーク上のNAS等のサーバ内蔵のストレージ以外を保管先に指定いる場合があります。

7)　データの復元

復旧用のデータからシステムが最後に正常にシャットダウンした時点のデータに戻すことが出来ます。
復元作業は当社の保守担当者が行うことが出来ます。

8)　システムの復元

OSの復元ポイントデータ

OSが保存する復元ポイントの状態に戻すことが出来ます。
復元作業は当社の保守担当者が行うことが出来ます。

サードパーティ製復元ツール

ツールを使って設置時のシステムイメージを保管しています。このイメージから設置時の状態に戻すことが出来ます。
復元作業は当社の保守担当者が行うことが出来ます。