S517-1132B

日付:2026年2月

発行:株式会社島津製作所　医用機器事業部

医用製品におけるサイバーセキュリティ対策方針

1.　当社の基本方針

当社製品をご利用いただき誠にありがとうございます。

株式会社島津製作所(以下「島津」)は、島津製品をサイバーセキュリティ上のリスクから継続的に保護するとともに、お客様を支援する各種サービスの提供や情報提供などの対策に努めます。お客様のネットワークの安全確保はお客様の責任とされています。島津は、お客様のセキュリティ管理担当者による安全確保のための活動を支援するため、お客様における安心・安全なネットワーク環境の維持のために必要と考えられる情報を提供するとともに、マルウェア(利用者の意図しない製品の動作を引き起こす悪意あるソフトウェア)やサイバー攻撃(不正アクセスによるデータ・プログラムの窃取、改ざん、破壊等)から島津製品を守る対策を継続的に提供することを目指しています。

2.　当社の提供するサービス

マルウェアやサイバー攻撃による島津製品への影響を最小にするために、島津は以下の予防措置をとるように努めます:

- システム・アクセスを許可された使用者だけに制限する機能を提供いたします。この機能を有効にすることにより、ユーザーアカウントとパスワード保護により限られた使用者のみが装置を使用することができるようになります。
- 新規納入時に、マルウェアやサイバー攻撃による影響を低減する設定を島津製品に行ないます。
- 島津製品に適用されているソフトウェアのアップデートは、検証した上で提供します。

  注記:　規格に対する適合や島津の品質規定に示された仕様を満たしていることを確認するため、ソフトウェアのアップデートをリリースする前に、広範囲なテストと確認を実施いたします。
- 検証後のソフトウェアアップデートを、検証されたアップデートプロセスに従って、島津に認定されたサービスマン(一部装置についてはお客様自身)によってのみ島津製品に適用します。

  注記:　ソフトウェアアップデートの条件は装置ごとの販売/保守契約の内容に基づき行われます。
- 島津デジタル製品では、製品毎にマルウェアやサイバー攻撃を防ぐルータまたはウイルス対策ソフトウェアパッケージ等の複数の対策を標準またはオプション(有償)として提供させて頂きます。

3. お客様における対策

お客様におかれましても、自らの施設に必要なマルウェアやサイバー攻撃の評価と、それらの脅威から自らを保護するために、可能な限りのあらゆる対策をおこなっていただく必要があります。

万が一、マルウェアやサイバー攻撃による装置の動作異常が疑われる場合は、装置の取扱説明書に従った処置を実施して下さい。その後、島津担当サービスに連絡をお願いします。

4. お客様の連絡をうけて

お客様の状況を確認させていただき、島津で実施出来ると判断する作業を実行させていただきます。

5. ソフトウェアのインストールについて

島津は島津が認定しないソフトウェアを、いかなる島津医用製品または他のいかなるシステムにもインストールしません。また、島津が認定しないソフトウェアのインストールから生じるいかなる性能への影響にも、島津は責任を負いません。そのようなソフトウェアのインストールは、製品保証が無効になるのみならず、システムに重篤な障害を与えたり、装置の使用や診断に重大な影響を与えたり、事故につながる場合がございます。

以下のような場合は、製品保証が無効となります。

- 島津が承認していないソフトウェア(ウイルス対策ソフトウェア含む)が製品にインストールされた場合
- 島津が認定していない作業員がソフトウェア(ウイルス対策ソフトウェア含む)のインストールを実施した場合

補足： マルウェアやサイバー攻撃対策について

マルウェアやサイバー攻撃には様々な手法が有りますが、主に以下の経路が利用されます。

経路1. マルウェアを含んでいる悪意あるメールやWEBページの閲覧

経路2. 装置またはシステムを構成するPC上でのマルウェアに感染したUSB・CD等のメディア上のプログラムの実行

経路3. 装置またはシステム内に攻撃者のPC等のデバイスを物理的に接続した攻撃

経路4. 外部からのネットワークを介した攻撃

上記に対して島津装置またはシステムでは、以下の対策を提供（またはお客様により実施）します。

経路1： 装置では原則としてこのような操作は行いません。リモート保守のために外部サーバに接続する場合にも、島津により安全が確認された保守用のサーバのみにアクセスを許可しています。

経路2： 島津が認定したサービスにより島津が安全を確認したメディアのみが保守に利用されます。お客様におかれましても島津が承認していないソフトウェアがインストール・実行されることがないように管理をお願い致します。

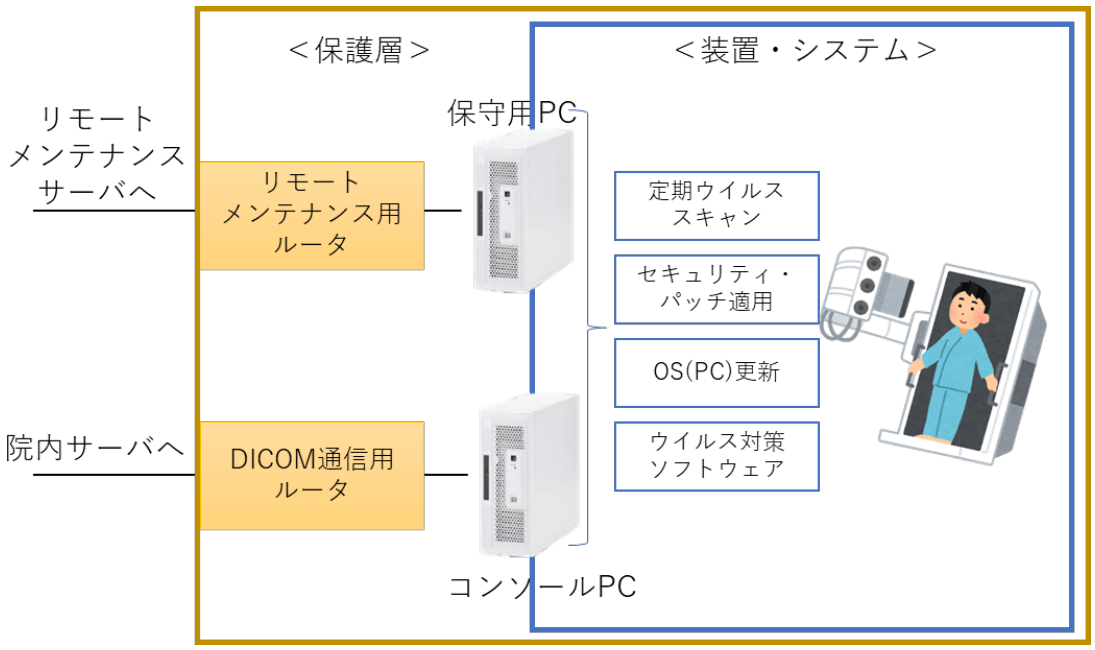
経路3： 島津装置またはシステムは通常アクセスが制限された部屋に設置または保管されることを前提にしています。部屋への入室管理はお客様の責任となります。

経路4： 島津装置またはシステムにおいて、最も想定される攻撃経路は本経路です。これに対し、島津はルータの設置、ウイルス対策ソフトウェアの導入、脆弱性対策など、単独またはこれらの組み合わせによる対策を提供します。

ネットワークを介した攻撃への対策の概要

昨今のランサムウェア攻撃などではマルウェアやサイバー攻撃は組み合わせて行われており、単一の対策に頼るのでは無く、以下のような複数の対策を階層的に組み合わせる多層防御により、サイバーセキュリティ上のリスクを効果的に低減することができます。

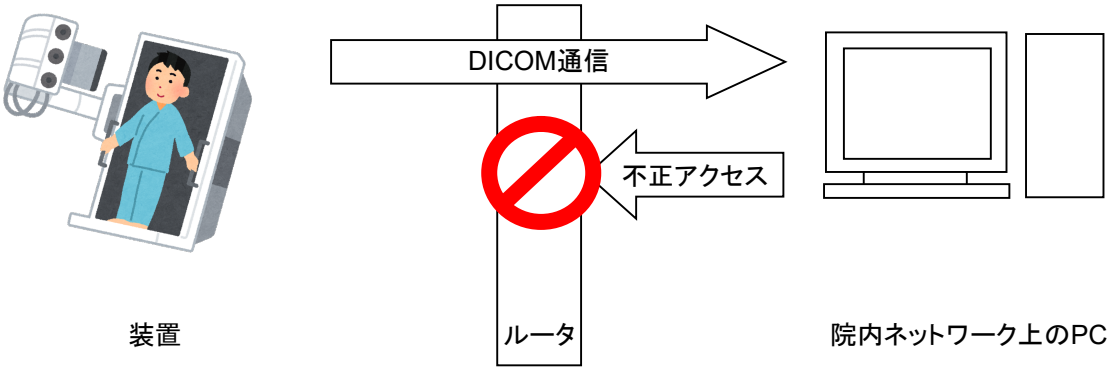
- 装置入口にルータを設置
- 装置にウイルス対策ソフトウェアを導入
- 定期ウイルススキャン
- サポート期間中のOS(PC)に更新
- セキュリティ・パッチ（最新F/W）適用



提供可能な手段は装置・システム毎に異なります。装置・システムの重要度やお客様のセキュリティ・ポリシーに合わせて、適切な対策を選択してください。

装置入口にルータを設置:

ルータ上のファイアーウォール機能を適切に設定し不要な通信を拒否することにより、ネットワーク経由の攻撃から装置を保護することができます。電子カルテ装置では、装置の扱う情報の重要性から、ルータによる保護を強く推奨します。



装置にウイルス対策ソフトウェアを導入:

装置に侵入したウイルスが意図しない動作を引き起こすことを防止するために、ウイルス対策ソフトウェアと呼ばれるソフトウェアを利用することが一般的です。ウイルス対策ソフトウェアについて、島津では一般的なブラックリスト型のウイルス対策ソフトウェアの他にホワイトリスト型のウイルス対策ソフトウェアも提供しており、装置の特性によりそのどちらかを採用しています。

＜ブラックリスト型ウイルス対策ソフトウェア＞

ブラックリスト型ウイルス対策ソフトウェアでは、パターンファイルに記載された特長を持つソフトウェアを検出することでシステムを保護します。

電子カルテ装置等の院外のサーバからパターンファイルを入手することが容易な装置ではブラックリスト型のウイルス対策ソフトウェアを使用しています。

＜ホワイトリスト型ウイルス対策ソフトウェア＞

ホワイトリスト型ウイルス対策ソフトウェアでは、安全が確認されているプログラムのみの実行を許可し、ウイルスに感染したプログラムを含む未知のプログラムの実行は許可しないことで安全性を担保しています。この仕組みのためパターンファイルは不要で、セキュリティ・パッチの提供されない旧バージョンのOSの装置でも安全に使用して頂けます。このため、インターネットに接続できないなどの理由でパターンファイルの入手が困難な多くの装置で使用されています。

定期ウイルススキャン:

ホワイトリスト型ウイルス対策ソフトウェア搭載装置は、ウイルスの発症はしませんがウイルスに感染する可能性があるため、ブラックリスト型ウイルス対策ソフトウェアでの定期的な検査を推奨します。

ウイルス対策ソフトウェア非搭載装置は、ウイルスの感染と発症の可能性が高いため、より高頻度での定期的な検査を推奨します。

サポート期間中のOS(PC)に更新:

OSのサポート期限を過ぎた場合には、脆弱性が発見された場合にも対策が提供されません。このため、装置のサイバーセキュリティ上のリスクは時間と共に増大します。この対策として後継OSに更新することが最も有効です。ただし、新しいOSは新しいH/Wが必要となることが多いため、多くのケースでPC単位での交換が必要となります。

サポートが終了になった装置等で後継のOS/PCが存在しない場合には、補完的対策として、ホワイトリスト型ウイルス対策ソフトウェアの搭載やルータによる保護が有効です。

セキュリティ・パッチ提供:

脆弱性が発見された場合には、セキュリティ・パッチと呼ばれる対策ソフトウェアのインストールを行うことが一般的です。医用装置の場合にはセキュリティ・パッチの投入には製造元の評価が必要になります。また、セキュリティ・パッチのインストールは教育を受けた作業者が行う必要があります。
セキュリティ・パッチの対応状況は装置やシステムにより異なりますので、必要な場合は担当サービスにお問い合わせください。

セキュリティ・パッチの提供が無い場合には、補完的対策として、ホワイトリスト型ウイルス対策ソフトウェアの搭載やルータによる保護が有効です。

なお、島津では装置やシステム毎にサポート期間中は、定期的にセキュリティ・パッチの適用の必要性を評価しています。

以上