S517-1132A

日付:2019年8月

発行:株式会社島津製作所　医用機器事業部

医用製品におけるウイルス対策方針

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(以降島津)は、危険なソフトウェア攻撃から島津製品を保護することに継続的に努め、かつお客様を支援するためにサービスを提供することを目指しています。お客様が可能な限りのセキュリティ対策について責任を持って実施していただく限り、島津は「コンピュータウイルスなどの使用者が意図しない製品の動作を引き起こす悪意のあるプログラムまたはソフトウェア」(以下ウイルス)から島津製品を保護することに継続的に努め、かつ、ウイルスに対するお客様のセキュリティ管理責任者によるセキュリティ対策への支援を目指しています。

2.　当社の提供するサービス

ウイルス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、ウイルスによる影響を最小に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、製品毎にウイルスの侵入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ウイルス対策の評価と、コンピュータウイルス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、ウイルス侵入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。この作業は保守契約内容に基づき行われます。

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： ウイルス侵入防止対策について

ウイルスは主に、以下の経路でPCに感染します。

経路1. ウイルスを含んでいる悪意あるメールやWEBページの閲覧

経路2. ウイルスに感染したUSB・CD等のメディア上のプログラムの実行

経路3. 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では、以下の対策を提供します。

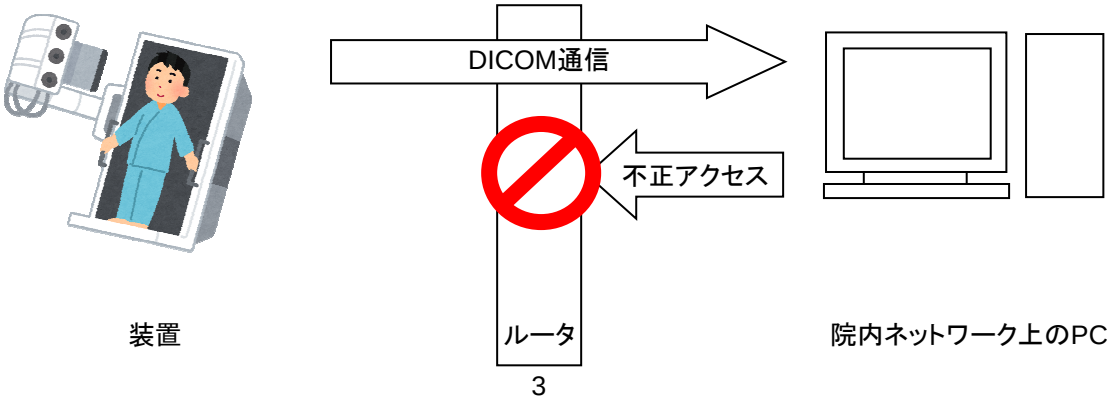
経路1： 装置では原則としてこのような操作は行いません。リモート保守のために外部サーバに接続する場合にも、島津により安全が確認された保守用のサーバのみにアクセスを許可しています。

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： 島津装置の通常使用時に経路1，経路2によってウイルス感染する可能性は極めて低く、経路3のネットワーク経由の攻撃で感染する可能性のみが残りますが、これに対してはルータまたはウイルス対策ソフトウェア、あるいはその組み合わせを提供致します。

ルータ：

ルータ上のファイアーウォール機能を適切に設定することにより、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、装置及び保守用サーバ全体をセキュアルータを用いて外部ネットワークから保護しています。



ウイルス対策ソフトウェア：

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、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。

以上