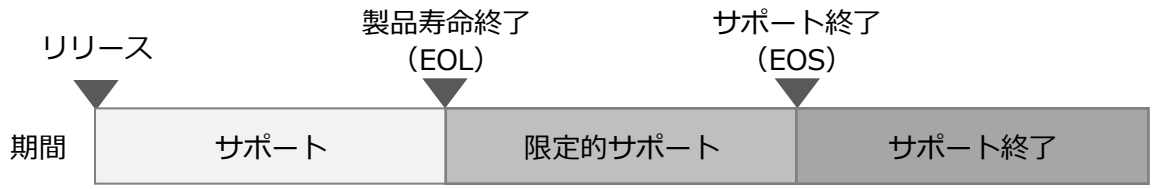
セキュリティ関連情報

1. EOL/EOS について

当該製品(FUJIFILM DIGIAL RADIOGRAPHY DR-ID 800）における EOL,EOS の定義を以下に示します。



＜EOL/EOS 方針＞
EOL（製品寿命終了）：＜本製品の EOL/EOS 情報＞に示します。
EOS（サポート終了）：当該機器の最終号機※1 の EOL から 1 年
※1 ソフトウェアのバージョンごとに管理されます。

＜本製品の EOL/EOS 情報＞

販売名	バージョン	製品寿命終了(EOL)	サポート終了(EOS)
DR-ID 800	すべて	設置から 5 年	当該機器の最終号機の EOL から 1 年

※本情報は必要に応じて変更されることがあります。

2．保守計画について

●サポート期間中（～EOL）

1) 脆弱性監視と対応

本製品における脆弱性を監視し、必要な修正を行い、セキュリティに関係するソフトウェアアップデート及び脆弱性修正の提供を行います。
また、メディカルシステム製品セキュリティ情報を Web サイトにて開示します。

2) セキュリティ更新

セキュリティ脆弱性対応について、当社が開発したソフトウェアの範囲において、脆弱性レベル、リスク分析等により当社が必要と判断した場合に、セキュリティアップデートを提供します。当社開発範囲外のソフトウェア（OS、OTS など）については、当社が必要と判断し、供給元よりセキュリティアップデートが準備された場合、提供します。
実際のセキュリティアップデートの適用作業は、保守契約／スポットサービス請負契約に基づきサービス作業を提供します。
Microsoft 社からリリースされる月例パッチの適用については、お客様からの要望によ

り、保守契約／スポットサービス請負契約に基づきサービス作業を提供します。

3) OS アップデート

OS のアップデートには対応しません。

本フェーズが搭載 OS のメーカーサポート期間を超える場合で、当社により補完的対策が必要と判断した場合に補完的対策を提供します。

●限定的サポート中（EOL～EOS）

1) 脆弱性監視と対応

本製品における脆弱性を監視し、必要な修正を行い、セキュリティに関係するソフトウェアアップデート及び脆弱性修正の提供を行います。

2) セキュリティ更新

セキュリティ脆弱性対応について、当社が開発したソフトウェアの範囲において、脆弱性レベル、リスク分析等により当社が必要と判断した場合に、セキュリティアップデートを提供します。当社開発範囲外のソフトウェア（OS、OTS など）については、当社が必要と判断し、供給元よりセキュリティアップデートが準備された場合、提供します。

実際のセキュリティアップデートの適用作業は、保守契約／スポットサービス請負契約に基づきサービス作業を提供します。

また、一般的な不具合等の解析依頼や修正については、当社により対応必要と判断した場合に対応します。

3) OS アップデート

OS のアップデートには対応しません。

本フェーズが搭載 OS のメーカーサポート期間に収まらない場合の補完的対策については保守契約／スポットサービス請負契約に基づき対応します。

4) EOS 通知

EOS の期日について、具体的な日程が確定し次第、Web サイトに掲載、または通知します。

●サポート終了後（EOS 以降）

1) 脆弱性監視と対応

市販後監視の一環として脆弱性情報を入手し、脆弱性評価を行い、記録を残します。

薬事上の回収（改修）に該当する場合を除き、脆弱性の修正を含むセキュリティアップデートの準備・提供は行いません。回収（改修）に該当しないが、製品に影響する深刻度が高い脆弱性（緊急性が高い脆弱性）については、情報を提供します。 また、情報提供を求められた場合は、セキュリティアドバイザリの開示を行います。

3．セキュリティインシデント発生時の対応

●サポート期間中（～EOL）、及び限定的サポート中（EOL～EOS）

1) セキュリティ更新

サイバーセキュリティ脆弱性が発見またはインシデントが検知された場合、製品への影響レベルにより、下記の通り対応を行います。
製品に影響する深刻度が高い脆弱性については、脆弱性の解説や製品への影響、暫定対策または恒久対策の提供日程を明らかにし、サービス実施会社を通じてすみやかに(遅くても、脆弱性の検知より 3 週間以内に）情報を提供します。脆弱性の検知より 7 週間以内に恒久対策を提供します。
製品に影響する深刻度が低い脆弱性については、次版リリース時に恒久対策あるいは補完的対策の評価を実施し、サービス実施会社を通じて情報を提供します。

2) インシデント発生時の対応

医療機関で情報セキュリティインシデントが発生した場合、医療機関との連携活動を含めた対応手順を以下のように定めています。
＜コンピュータウイルスの発生が医療機関内の機器（他社製品を含む）で確認された場合＞
① サーバー機器・院内端末の LAN ケーブルを抜線し、院内 LAN から分離する。併せてリモート用 VPN ルータが設置されている場合、WAN 側の LAN ケーブルを抜線する。
② 被害状況の確認（コンピュータウイルスの種類確認）を行い、現状を保全する。
③ 医療機関のセキュリティ管理者と連絡を取り、情報共有及び対応についての指示を受ける。
必要に応じて、サービス実施会社が、医療機関と以下の情報を共有することを指示します。

- インシデント対応中にサービス実施会社が順守すべき事項
- インシデント発生時の連絡先及び対応手順
- 復旧の際に必要となる、医療機器の設定情報やアカウント権限の付与

3) 復旧

サービス実施会社を通じて、インシデントの発生前の通常の運用状態に戻すための復旧の機能及び手順の情報を提供します。

●サポート終了後（EOS 以降）

製品をご利用いただいている環境でセキュリティインシデントが発生した場合、装置への影響の有無にかかわらず、一旦ネットワークから切り離してください。インシデントが解決し、ネットワークに異常がない状態になってから、再接続をお願いします。
なお、当社の製品の動作に異常がある場合には、異常の状態を分かる範囲で当社までご連絡ください。

以上