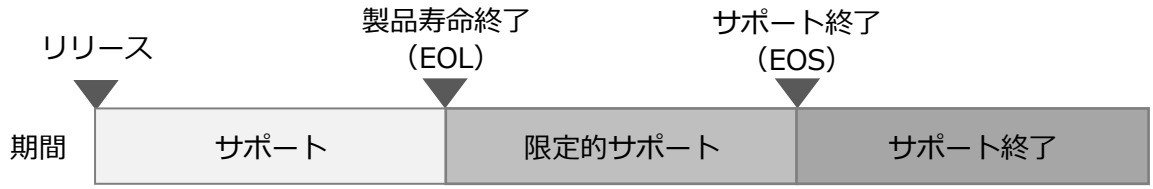
セキュリティ関連情報

1. EOL/EOS について

当該製品（SYNAPSE LEAD/SYNAPSE LEAD Cloud）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)：インストールした H/W の耐用期間に準ずる。

・EOS(サポート終了)：バージョンの製造販売終了後から 8 年

※本情報は必要に応じて変更されることがあります。

＜本製品の EOS 情報＞

上記方針に基づき、EOS が確定したバージョンについて記載します。

※1:EOL については、当該製品をご購入された時期に応じて、お客さまごとに異なりますので、詳しくは担当営業にご確認ください。

※2:何らかの事情により日程が変更になった場合は、その旨を事前に通知いたします。

販売名	バージョン	サポート終了(EOS)
SYNAPSE LEAD/ SYNAPSE LEAD Cloud	1.1	2034 年 4 月
	1.2	EOS 日程が確定次第掲載いたします。

2. 保守計画について

●サポート期間中（～EOL）

- 対応が必要な脆弱性に対し、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。
- 実際の適用作業は、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。

●限定的サポート中（EOL～EOS）

- 対応が必要な脆弱性に対し、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。
- 実際の適用作業は、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。

・ 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。

●サポート終了後（EOS 以降）

・ 市販後監視の一環として脆弱性情報を監視しますが、薬事上の回収（改修）等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。セキュリティに関する責任はお客さまへ移転されます。
・ 回収（改修）に該当はしないものの、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。
・ その他、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。
・ SYNAPSE LEAD Cloud について、バージョンアップを適用しない場合は、お客さまとの調整の上、クラウドとの接続を遮断させていただく場合がございます。

3．セキュリティインシデント発生時の対応

セキュリティインシデント発生時には、以下のご対応をお願いいたします。

(1) 初期対応（ネットワークからの切り離し）

当社製品が接続されたネットワーク内で、セキュリティインシデントが発生した、またはその疑いがある場合、当社製品をネットワークから切り離してください。
また、当社製品が搭載された機器の電源は切らないでください。また、当社製品をアンインストールしないでください。

(2) 状況の把握・サービス担当者への連絡

以下の A～F の観点で、被害の範囲や状況を可能な範囲で確認し、サービス担当者に、これらの情報のご提供をお願いします。

A. 本製品の設定情報の不正な変更
B. 診断・治療に対する不正な変更又は無効化
C. 機密データの喪失、改竄又は開示
D. 本製品の機能停止、誤動作又は不正動作
E. 他の機器・システムへの拡散
F. マルウェア感染の疑い

(3) 措置・復旧

医療機関内の管理者の判断に基づき、サービス担当者と連携して、ウィルススキャンやマルウェア除去等の適切な措置を行ってください。当社製品が正常に動作することを確認した後、管理者の判断により、ネットワークへ再接続して、製品の使用を再開してください。

以上