

オリンパス株式会社

2026 年 9 月 14 日

システムコントローラー UCES-4 セキュリティサポート終了に関するご案内

対象製品名: システムコントローラー

対象モデル名: UCES-4

お客様各位

拝啓 時下益々ご清栄のこととお慶び申し上げます。また日頃より格別のご高配を賜り、厚く御礼申し上げます。

このたびシステムコントローラー UCES-4（以下、UCES-4）のソフトウェアで使用するオペレーティングシステム（以下、OS）のサポート終了に伴い、本通知をさせていただくこととなりました。本件はセキュリティ対策に関連する内容であるため、貴施設のシステム管理者様ともご連携のうえ、ご対応をご検討いただけますと幸いに存じます。

お客様にはご不便をおかけいたしますが、事情ご監察のうえ、何卒ご理解賜りますようお願い申し上げます。

敬具

記

セキュリティサポートの終了について

このたび、UCES-4 に搭載している OS について、部品供給会社からのサポートが終了することとなりました。これにより、将来的に新たなセキュリティ脆弱性が発見された場合において、弊社から OS のセキュリティパッチをご提供できなくなりますことをご了承願います。

弊社は、製品の安全性およびセキュリティの重要性を十分に認識し、継続的な向上に努めております。本製品のセキュリティ脆弱性についても継続的に監視を行っており、本通知時点において、本製品に影響を与えるような重大な脆弱性は確認されておりません。また、本製品を標的としたサイバー攻撃も確認されておりません。

なお、本製品に影響を及ぼす重大な脆弱性の悪用が確認された場合には、リスクを評価した上で、推奨される対応措置について弊社ウェブサイトでの公表、または各ご施設へ直接、情報提供を行います。

弊社は、本製品の修理サービス期間が満了するまでの間、修理などのハードウェアサポートは引き続き提供いたします。また、必要に応じて、機能性維持（例：他製品との組み合わせの保証など）のため、OS サポート終了の影響を受けないソフトウェアの更新を提供いたします。

UCES-4 の将来的なサイバーセキュリティリスク軽減に向けた推奨事項

IMDRF（International Medical Device Regulators Forum）の医療機器サイバーセキュリティに関するガイダンスにも記載されているとおり、医療機器製造業者およびヘルスケアプロバイダは、医療機器のセキュリティ確保において共同の責任を担っています。

弊社では、医療機器を不正アクセスから適切に保護するために、お客様施設においてアクセス制御の仕組みの整備、ユーザー手順の徹底、およびトレーニングの実施など、サイバーセキュリティに関するベストプラクティスを継続的に実施いただくことを推奨しております。

つきましては、以下の対応をご検討いただけますと幸いです。

- ネットワーク接続について

パブリックネットワークおよび院内ネットワークへ接続されていないことをご確認ください。本製品はネットワーク接続を想定した仕様とはなっておりません。

- USB ポート（MEMORY 端子、SYSTEM 1 端子、SYSTEM 2 端子）の物理的保護

専用のキーを使用しないと取り外せないポートロック（例：SmartKeeper 社製 USB ポートロック、モデル番号：UL03 または同等品）を製品前面のおよび背面の USB ポート（MEMORY 端子、SYSTEM 1 端子）、Powered USB ポート（SYSTEM 2 端子）に差し込むことを推奨いたします。ケーブルが差し込まれている場合は、ポートとケーブルの接続部に、取り外し時に改ざんの痕跡が残るセキュリティステッカー（例：サンワサプライ製 セキュリティステッカー〔型番：200-SL007〕または同等品）を貼付することを推奨いたします。

- LAN ポート（SYSTEM I/F 1～6 端子）の物理的保護

専用のキーを使用しないと取り外せないポートロック（例：SmartKeeper 社製 LAN ポートロック、モデル番号：NL03 または同等品）を製品背面の通信端子（SYSTEM I/F 1～6 端子）端子に差し込むことを推奨いたします。

最新の製品セキュリティ情報につきましては、定期的に弊社ウェブサイトの「製品セキュリティ」ページをご確認いただくことを推奨いたします。

ご質問やご不明な点がございましたら、オリンパス内視鏡お客様相談センターまたは最寄りの支店までお問い合わせください。

以上