PHILIPS

2025 年 12 月

株式会社フィリップス・ジャパン

IntelliSpace Cardiovascular のセキュリティ情報に関するお知らせ

Security Advisory の ASP.NET Core Advisory (CVE-2025-55315) (2025 November 5)の公開内容に関しまして、高い深刻度の脆弱性が報告されているため、翻訳と共に日本国内のお客様向けに周知させていただきたい情報をお伝えいたします。

< ASP.NET Core Advisory (CVE-2025-55315)の翻訳>

公開日：2025 年 11 月 5 日

更新日：2025 年 11 月 14 日

フィリップスは現在、ASP.NET Core に影響する最近公表されたセキュリティ機能の回避の脆弱性（CVE-2025-55315）に関連する動向と更新情報を監視しています。本脆弱性が悪用された場合、認証済みの攻撃者が巧妙に作成した HTTP リクエストをウェブサーバーに送信でき、機密データへの不正アクセス、サーバーファイルの改ざん、あるいは限定的なサービス拒否（DoS）状態を引き起こす可能性があります。

フィリップスは、弊社の製品セキュリティポリシーと手順の一環として、フィリップス製品とソリューションが脆弱性の影響を受ける可能性について継続的に評価を行い、対策の検証を行っています。

フィリップスは、フィリップスが承認する製品仕様内で導入・運用される際の製品の安全性、セキュリティ、整合性、および規制遵守の確保に取り組んでいます。そのため、フィリップスのポリシーおよび規制要件に則り、フィリップス製品に対するすべての設定変更やソフトウェアの適用（オペレーティングシステムのセキュリティ更新やパッチを含む）は、フィリップス製品固有の検証・妥当性確認を行い、承認・周知されたお客様向け手順書またはフィールド対応に限定して行われます。

契約対象のお客様は Philips InCenter をご利用いただけます。Philips InCenter のアクセスを要求し、掲示されている製品固有の情報をご参照いただくことを推奨いたします。契約の有無に関わらずご不明点があるお客様は、お使いの製品に関する最新情報について、カスタマーケアセンターにお問い合わせください。

フィリップスは、お客様が本脆弱性の影響を受ける可能性のある製品を特定できるよう、以下の製品リストを提供しています。リストに記載のない製品は影響を受けないものとご判断ください。追加の製品が判明した場合、フィリップスは随時リストを更新いたします。

867113 – Focal Point 2.x[1] （注 1）　　830089 – IntelliSpace Cardiovascular (8.1)[2] （注 2）

上記の全製品に対し、フィリップスは最善の緩和策を評価しています。具体的な緩和策は以下のとおりです。

[1] InCenter に情報またはパッチが掲載されています。

[2] ソフトウェアのみの製品で、お客様が所有するオペレーティングシステムを使用する場合、適用可能な緩和策を実施する責任はお客様にあります。

（注 1）　Focal Point は日本では販売・導入されておりません。

（注 2）　本脆弱性は IntelliSpace Cardiovascular サーバー（ウェブサーバーも含む）に限定されます。

＜国内のお客様向けの周知＞

日本国内のお客様におきましては、本脆弱性の潜在的なリスクを最小限に抑えるため、弊社は以下の緩和策を推奨します：

- IntelliSpace Cardiovascular サーバーのネットワークへの露出を最小限に抑え、インターネットからアクセスできないようにする。
- IntelliSpace Cardiovascular サーバーの配置されている医療情報ネットワークをファイアウォールの背後に配置し、他の業務系ネットワークから分離する。
- IntelliSpace Cardiovascular サーバーへリモートアクセスを要する場合は仮想プライベートネットワーク(VPN)のようなより安全な手段を使用し、VPN のソフトウェアを利用可能な最新バージョンに更新する。また VPN の安全性は、接続機器の安全性と同程度のみであることを認識する。

以上