

Devices

Security by Design

GE HealthCareの医療機器における
サイバーセキュリティ対策



はじめに

GE HealthCareでは、“DEPS(Design Engineering for Privacy and Security: プライバシーとセキュリティのための設計工学)”を含む厳格な製品開発プロセスを採用しています。DEPSは、すべての製品に対して設計段階からのセキュリティ対策を含むプライバシーおよびセキュリティリスク評価を実施し、ユーザーマニュアルへの対策の記載や、医療機器セキュリティに関する製造者開示文書(MDS2)の提供を通じて、製品のセキュリティリスクに効果的に対応します。また、このプロセスには、保護対象保健情報(PHI)および個人情報(PI)を保護するためのセキュリティ対策も含まれています。

GE HealthCareの製品は、米国および世界の多くの市場で商業的に提供されており、各国のプライバシー関連法規(1996年制定のHIPAAを含む)への準拠を支援するための管理策を設計・実装しています。GE HealthCareは、プライバシー影響評価(Privacy Impact Assessment)およびセキュリティリスク評価(Security Risk Assessment)を実施する正式なプロセスを導入しており、NIST 800-53、ISO 27000、HIPAA、EU MDRなどの規格や法規に基づいたセキュリティ管理策を適用しています。当社のデバイスは、適切な運用上のセキュリティ管理策が整った環境で使われることを前提に設計されています。GE HealthCareは、プライバシーおよびセキュリティはお客様との「共有責任」であると考えており、製品が使用される物理的および技術的な環境を考慮した対応を行っています。

いかなるシステムも100%リスクを排除することはできませんが、GE HealthCareの麻酔装置には、以下のリスク低減対策が組み込まれています。

- 麻酔器に搭載されているオペレーティングシステム(OS)は、市販の一般的な汎用OSではなく、麻酔器向けに特別に設計・強化された専用システムを採用しており、安全性と信頼性を高いレベルで確保しています。また、Carestation 600シリーズV2では、OSにLinuxやNucleusを採用しています。
- 管理的セキュリティコントロールによりシステム内のファイルが不正に改ざんされることを防止しています。
- 本装置には、機密性の高いデータや患者情報は一切保存されない設計となっています。
- PHI/PI(保護対象医療情報/個人情報)の使用は初期設定で無効化
- 認証されたユーザーが機能を有効にした場合に限り、収集されたPHIおよびPIは暗号化されることなく、平文でネットワーククライアントに送信されます。
- GE HealthCareでは情報セキュリティおよびプライバシー保護体制の妥当性を確認するため、定期的にサイバーセキュリティの侵入テストを実施しています。

ネットワーク接続機能を備えた唯一のシステムとして、Aisys™ CS2麻酔システムには、上記に加えて以下のような制御機能も備わっています。

- すべてのオープンポートはユーザーが設定可能であり、ポートは不正アクセスや異常な通信を検知するために常時モニタされています

よくあるご質問 (FAQ)

構成とハードニング

麻酔器のソフトウェアはどのようにセキュリティ強化されていますか？

- ・ 麻酔器の動作に必要な機能だけを搭載した、専用設計のOS(Windows、Linux、Nucleus)を採用しています。
- ・ システムメモリは二重ストレージ構成により保護されており、データの信頼性と復元性を確保しています。
- ・ キーボードやマウスの操作は無効化されており、シェルやコマンドプロンプトなどへの不正アクセスを防止しています。
- ・ システムソフトウェアは、インストール時にGEヘルスケアの電子署名によって正当性が認証されます。さらに、起動時および運用中にも継続的に整合性が検証され、不正な改ざんや未承認の変更を防止します。



Aisys™ CS2とCarescape Canvasモニターとの連携

Aisys CS2麻酔システムでは、ネットワークモニターがポートの通信状況を監視しており、異常が検出された場合には自動的に該当ポートを無効化します。初期設定ではネットワーク通信は無効化されており、使用者が明示的にネットワーク接続を設定しない限り、通信は行われません。通信を有効にした場合でも、システムからはあらかじめ許可された(ホワイトリストに登録)ネットワーク機器とのみ通信が行われます。

Aisys CS2 麻酔器では、リカバリー機能(Recourse and Recovery)により、ディスプレイシステムに障害が発生した場合でも換気機能がサブシステムによって維持され、麻酔の継続が確保されます。ディスプレイは自動的に再起動して復旧を図りますが、その間も換気は中断されません。

ディスプレイシステムが復旧した後は、さらなる障害を防ぐためにネットワーク通信は自動的に無効化されます。通信を再開するには、システムを手動で再起動する必要があります。

インバウンド(外→内)通信はどのように保護されていますか？

- ・ シリアル通信は、以下の目的に限定してサポートされています：
 - 臨床データを、互換性のある他のベッドサイド機器へ送信するため
 - サービスユーザーによる認証後、サービスモードにおいてシリアルポート経由のサービス通信を有効にするため
- ・ USBメディアは、"スーパーユーザーモード"および"サービスモード"においてのみ使用可能であり、設定管理、ソフトウェアのアップグレード、ログ管理の目的に限定されます。

- ・ ネットワーク通信は、Aisys CS2 麻酔器においてのみサポートされており、以下の目的に限定されています：
 - 臨床データを、SBX/HL7に対応した最大4台のクライアント機器へ送信するため
 - システムがスタンバイモード中に、ログデータをFTPサーバーへ送信するため
 - スタンバイモード中に、ネットワークタイムサーバーと時刻を同期するため
 - ネットワークからのDoS（サービス拒否）攻撃が検出された場合、ネットワークポートを無効化するか、障害から復旧後にその症例中はネットワークポートを無効化して通信を遮断するため

ネットワークや外部メディアからの自動実行や起動から、システムはどのように保護されていますか？

本システムは、GE HealthCareが提供する専用USBメモリからのみ外部メディアによる起動が可能であり、そのUSBはGE HealthCareの認定担当者のみが所持しています。さらに、GE HealthCare社製の麻酔器が設置されている手術室は、認可された関係者のみが立ち入れる制限区域となっています。

麻酔装置は、ソフトウェアの改ざんをどのように防止していますか？

本装置は、GE HealthCareが提供するUSBメモリに格納されたGE HealthCare社製ソフトウェアのみを受け入れることができます。システムソフトウェアのインストール前には、バイナリ署名および互換性のチェックが行われます。さらに管理上の対策として、本麻酔システムは手術室や、内視鏡室、カテーテル検査室、CT/X線検査室などの非手術室環境に設置されており、これらは原則として認可された医療従事者のみが立ち入れる制限区域です。

通信中のデータおよびデータ保護

麻酔器のソフトウェアはどのようにセキュリティを強化されていますか？

麻酔器は、機密性の高い個人情報や保護対象となる医療情報を保存しません。患者の体重や年齢などの情報を一時的に使用する場合がありますが、これらの情報は装置の電源を切るか、新たな症例を開始した時点で自動的に削除されます。

麻酔器はランサムウェア攻撃からどのように保護されていますか？

麻酔器は、症例終了後に機密性の高いデータを保持しないため、ランサムウェア攻撃のリスクは基本的に該当しません。また、システム設定はUSBメモリにエクスポートして保存することができ、必要に応じて他の麻酔器にインポートすることで、同一の設定を一括で復元することも可能です。

通信中のデータはどのように扱われていますか？

シリアルポートから出力されるデータは暗号化されていません。このデータストリームには、装置からの測定値や設定値などの瞬時データが含まれていますが、患者を特定できるような個人情報は一切含まれていません。



Carestation 750麻酔システムと
CARESCAPE Canvasシリーズの組み合わせ

Aisys CS² 麻酔システムでは、患者氏名やID番号などの個人を特定できる情報の使用は、初期設定では無効化されています。これらの情報を使用するには、"スーパーユーザー設定メニュー"にてスーパーユーザーが明示的に有効化する必要があります。有効化された場合、患者データはネットワーククライアントに平文(暗号化されていない形式)で送信されます。そのため、使用を検討する際は、ネットワークの制御状況やリスクを十分に確認・評価したうえで、有効化するかどうかを判断することが推奨されます。

悪意のある第三者が通信を傍受し、データを改ざんする可能性はありますか？

Aisys CS² 麻酔システムでは、データは標準的な暗号化されていない HL7 形式、または GE HealthCare 独自の暗号化されていない SBX 形式で送信されます。本装置は外部からのデータ受信を行わず、データは一方向にのみ送信されるため、中間者攻撃(Man-in-the-Middle)によって本装置機能が影響を受けることはありません。ただし、麻酔記録システムや電子カルテに送信されるデータが、第三者によって改ざんされる可能性があり、記録内容に影響を及ぼすリスクがあります。そのため、ネットワークへの不正アクセスや悪意ある行為を防ぐための適切なセキュリティ対策を講じることが推奨されます。

ペネトレーションテスト(侵入テスト)

安全制御はどのように検証されましたか？

GEヘルスケアは、第三者機関に依頼し、USB、シリアル、ネットワークポートの脆弱性を特定するため、ペネトレーションテスト(倫理的ハッキング)を通じてシステムおよびセキュリティ制御のストレステストを実施しました。このテストでは、パシエントケアに影響を及ぼすような脆弱性は確認されませんでした。また、第三者機関からの提言は、今後の製品開発において考慮される予定です。

DoS(サービス拒否)攻撃はシミュレーションされましたか？

Aisys CS²麻酔システムはDoS攻撃にどう反応しますか？

ペネトレーションテストの一環として、DoS(サービス拒否)攻撃が実施されました。ネットワークモニターが異常な通信量の増加を検知した場合、システムを保護するために通信ポートは自動的に無効化されます。仮にDoS攻撃によってディスプレイシステムがクラッシュした場合でも、リカバリー機能により換気機能はサブシステムによって維持され、ディスプレイシステムは自動的に再起動して復旧を試みます。ディスプレイが復旧した後も、さらなる障害を防ぐためにネットワーク通信は無効化されたままとなり、ユーザーが手動でシステムを再起動するまで通信は再開されません。



Carestation™ 650 麻酔システムと
CARESCAPE™ B1x5 モニターの組み合わせ

オペレーティングシステムの健全性

「オペレーティングシステムがサポートされている」とはどういう意味ですか？「延長サポート」とは何ですか？

サポートされているオペレーティングシステム(OS)とは、ソフトウェア開発元(例：Microsoft)がサイバーコミュニティおよび自社製品を継続的にモニタしている状態を指します。脅威が特定され、CVE(共通脆弱性識別子)データベースに正式に登録された場合、開発元はその脆弱性を修正するパッチを提供することを約束します。セキュリティ脆弱性はその深刻度に応じて評価されます。製品の標準的なサポート期間が終了すると、Microsoftは「延長サポート」という追加フェーズを実施し、この期間中は「Critical」と分類されたCVEに対してのみ修正を提供することを約束します。

既存のGE Healthcare社製麻酔装置に、すべてのMicrosoftパッチは適用されますか？

本麻酔システムでは、強化されたソフトウェアおよび専用に構成されたオペレーティングシステムにより、すべての脆弱性(CVE)が直ちに麻酔ソフトウェアの脆弱性に該当するわけではありません。CVE(共通脆弱性識別子)が報告された場合、エンジニアリングチームが関連文書を精査し、その脆弱性が本システムに影響を及ぼすかどうかを評価します。Microsoft®のソフトウェアパッチについても、麻酔器のソフトウェアに関連するもののみを適用しています。

OSがサポートされていない/延長サポート期間を過ぎている状態とは？

Microsoftの「サポート終了日」または「延長サポート終了日」を過ぎると、ベンダーは脆弱性の修正を行う義務を負わなくなり、GE HealthCareのような企業に対しても、バグや脆弱性の対応支援を提供しなくなります。

サポートされていないOSを使用すると、システムが危険化されますか？

OSのサポートが終了したからといって、システムが直ちに危険にさらされるわけではありません。技術的および管理的な対策は引き続き有効です。脆弱性が見つかる可能性は、OSがサポートされているかどうかによって変わるものではありません。主な違いは、脆弱性が発見された際に取れる対応策の選択肢にあります。

OSがサポートされていない場合、GE HealthCareはどのようにして脆弱性を把握するのですか？

一部の製品については、Microsoftは「拡張セキュリティ更新プログラム」のもとで、拡張サポート終了後モニターを継続しています。さらに、特定の脆弱性は、サポート中のOS製品とサポート終了後の製品の両方に影響を及ぼすことがあるため、そのような場合にはサポートが終了したOSであっても、発見された脆弱性に関する通知を受け取ることがあります。

第三者が脆弱性を発見した場合、複数存在する脆弱性データベース（例：<https://nvd.nist.gov/>）のいずれかに報告することができます。GE HealthCareは、脆弱性管理プロセスを通じて、こうした情報を把握します。これは、Microsoftが自社製品の脆弱性を把握する方法と同様であることが多いです。

脆弱性が一般には公開されておらず、ダークウェブ上でハッカーの間だけで共有されている場合、たとえMicrosoftの監視体制であっても、その脆弱性が悪用されるまで検知できない可能性があります。

WEC(Windows Embedded Compact)2013で脆弱性が見つかった場合はどうなりますか？

WEC2013に関する脆弱性が特定された場合でも、それがGE HealthCareの麻酔装置に直ちに影響を及ぼすとは限りません。私たちのプロセスの第一歩は、自社のソフトウェアを評価し、その脆弱性が該当するかどうかを確認することです。

既存のOS(例：WEC 2013)において、これまでに発見された脆弱性の数は？そのうち、実際に適用されたパッチの数は？

GE HealthCareでは、サードパーティ製ソフトウェアコンポーネントに関して報告された脆弱性を定期的に確認し、それがシステムの機能や患者の安全性に与える影響を評価しています。これまでのところ、製品の機能や患者安全に影響を及ぼすような脆弱性や異常は、サードパーティ製ソフトウェアにおいて確認されていません。

脆弱性が麻酔装置のOSに存在し、かつそのコンポーネントが実際に使用されている場合、どうなりますか？

万が一、特定の脆弱性が本システムに該当し、既存の制御策では不十分と判断された場合でも、GE HealthCareは製品のサポートを継続し、状況に応じた対応計画を速やかに策定・実施いたします。

Summary

悪意ある攻撃者による医療システムへの脅威は拡大を続けており、現在では麻酔器や集中治療室の人工呼吸器などのクリティカルケア機器も標的となっています。

GE HealthCareの麻酔器関連機器は、製品のセキュリティリスクに対応するために厳格な設計プロセスを経て開発されており、高い耐障害性を備えるように設計・強化されています。

患者および操作する医療従事者の安全を最優先に、GE HealthCareの麻酔器は、標準的なオペレーティングシステムをカスタマイズしたバージョンやLinux、Nucleusを採用し、不要なコンポーネントを排除することで、一般的な脆弱性の影響を受けにくい設計となっています。

これらのシステムには、次のような複数のセキュリティ層が追加されており、1) 不要なアクセスの制限、2) 外部からの通信の削減と保護、3) 治療機能に影響を及ぼす可能性のあるサイバー攻撃のリスク低減を目的としています。

GE HealthCareは、医療機関が求める高い基準を満たし、さらにそれを上回ることを目指しており、そのために各ソリューションは第三者機関によるストレステストを通じて評価・検証されています。

セキュリティ技術の状況は常に進化を続けていますが、GE HealthCareの製品もそれに合わせて進化を続けています。

販売名 : エイシス(エイシスCS²の薬事販売名はエイシスです)
承認番号 : 21900BZX007000
販売名 : Carestation 750シリーズ
承認番号 : 30200BZX00223000
販売名 : Carestation 600 シリーズ
承認番号 : 22700BZX00422000
販売名称 : CARESCAPE ベッドサイドモニタ Canvas シリーズ
認証番号 : 305ADBZX00092000

GE HealthCareは、本資料に記載されている仕様および機能を予告なく変更、または製品の販売を中止する権利を有します。

Carestation、Aisys、CARESCAPEはGEHealthCareの商標です。Linuxは、米国およびその他の国におけるLinus Torvaldsの登録商標です。Nucleusは、Mentor Graphics Corporationの米国ならびに他の国における登録商標です。WindowsおよびMicrosoftは、Microsoftグループの商標です。

GE HealthCareの事前の書面による許可なしに、本資料のいかなる形式での複製も禁止されています。

本資料の内容は、病気や症状の診断・治療に使用することを目的としたものではありません。読者は必ず医療専門家に相談してください。

製品はすべての国や地域で提供されているわけではありません。詳細については、GEヘルスケアの担当者までお問い合わせください。

Aug 2025

JB12718JA



GE HealthCare