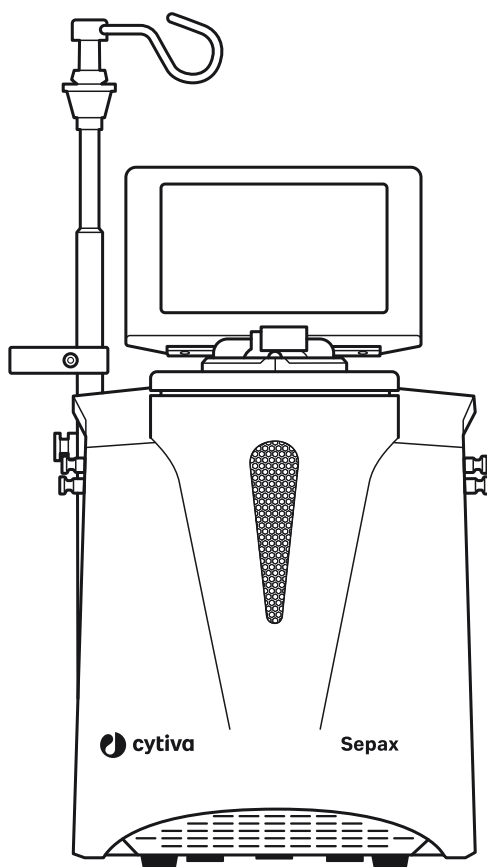


# Sepax™ S-100, Sepax™ 2 RM, and Sepax™ C-Pro

GMAP 5.5.x

## プライバシーとセキュリティに関する マニュアル

英語から翻訳



## 目次

<b>1</b>	<b>はじめに .....</b>	<b>3</b>
<b>2</b>	<b>プライバシーとセキュリティの環境 .....</b>	<b>5</b>
<b>3</b>	<b>認証、認可、監査ログの取得 .....</b>	<b>7</b>
3.1	アクセスコントロール .....	8
3.1.1	ID のプロビジョニング .....	9
3.1.2	パスワード .....	11
3.1.3	ユーザー認証 .....	12
3.1.4	アクセス権の割り当て .....	13
3.2	監査ロギングとアカウントビリティコントロール .....	16
<b>4</b>	<b>被検者プライバシー同意の管理 .....</b>	<b>18</b>
<b>5</b>	<b>情報の保護 .....</b>	<b>19</b>
5.1	キオスクモード .....	20
5.2	有線ネットワークのセキュリティ .....	21
5.3	無線ネットワークのセキュリティ .....	22
5.4	リムーバブルメディアのセキュリティ .....	23
5.5	保存データのセキュリティ .....	25
5.6	バックアップに関する注意事項 .....	26
5.7	データ完全性 .....	27
5.8	データ保持ポリシー .....	28
5.9	データ破壊ポリシー .....	29
<b>6</b>	<b>システムの保護 .....</b>	<b>30</b>
6.1	悪質なソフトウェアからの保護 .....	31
6.2	システム変更の管理 .....	32
<b>7</b>	<b>リモートアクセス .....</b>	<b>33</b>
<b>8</b>	<b>本製品により収集された個人情報 .....</b>	<b>34</b>
<b>9</b>	<b>製品セキュリティ補足資料 .....</b>	<b>35</b>

# 1 はじめに

## 本書について

本マニュアルでは、Sepax™ S-100, Sepax 2 RM, and Sepax C-Pro の使用におけるプライバシーとセキュリティの留意事項について説明します。

## 本マニュアルの目的

本マニュアルでは、Sepax S-100, Sepax 2 RM, and Sepax C-Pro の用途、搭載されているプライバシー機能とセキュリティ機能、本製品の適切な設定方法と使用方法について説明します。

## 本マニュアルの適用範囲

本マニュアルはソフトウェアバージョン GMAP v5.5.x に適用されます。

## プライバシーとセキュリティの概要

本マニュアルは、プライバシーとセキュリティの概念を読者が理解していることを前提としています。セキュリティによって、機密性、完全性、可用性に対するリスクからシステムと情報の両方が保護されます。セキュリティとプライバシーを連携させることによって、リスクを許容レベルに抑えることができます。医療の現場では、本製品の用途と関連したプライバシー、セキュリティ、および安全性のバランスを保つ必要があります。

お客様は、リスク管理手順を使用して、プライバシーとセキュリティとセーフティのリスクを評価し、優先順位をつけることができます。リスク管理の使用を通じて、本製品の機能を最大限に生かす方法を見極めることができます。

## 製品の用途に関する重要なユーザー情報

Sepax S-100 システムは、血液、血液製剤、細胞生成物を対象とした細胞処理システムで、互換性のある使い捨て分離キットとのみ組み合わせて使用することを目的としています。加工品は、医療用として過去に回収されたものです。Sepax S-100 本体では、遠心分離による細胞分離と処理が可能です。この医療機器は、ドナーまたは患者に接続されていません。

Sepax C-Pro 細胞処理システムは、細胞治療製品の製造のために細胞処理用として開発された技術であり、自動化され、機能的に閉鎖されています。これは Sepax C-Pro 専用のソフトウェアプロトコルおよびキットとの組み合わせで細胞生成物を処理するよう設計されています。本システムは、集積、磁気ビーズ培養、スピノキュレーション、濃縮、洗浄、希釈、分離などといった複数の処理ステップの多様な組み合わせを実現します。Sepax C-Pro は、ヒトの治療または診断を目的とした使用を想定していません。適合する Sepax C-Pro ソフトウェアプロトコルおよびキットのみを併用してください。

## 医療機器製品の用途に関する重要な ユーザー情報 (米国向け)

Sepax S-100 システムは、臍帯血細胞処理システムで、Biosafe の支給品で互換性のある使い捨て分離キットのみと組み合わせて使用することを目的としています。処理する臍帯血は、医療用としてあらかじめ収集されたものを使用します。

Sepax 2 RM システムは、さまざまな細胞生成物 ( 骨髄、アフェレーシス、末梢血、これらと同様の希釈成分など ) から遊郭細胞を分離することを目的とする細胞処理システムです。

Sepax S-100 システムと Sepax 2 RM システムは、再現可能な臍帯血高速自動分離を可能にします。Sepax S-100 システムと Sepax 2 RM システムは、血液が被検者と Sepax S-100 または Sepax 2 RM ユニットの間を直接循環する輸血用途 ( ベッド脇 ) での使用を目的としていません。

## 連絡先情報

プライバシーとセキュリティに関するお問い合わせは、[cytiva.com/contact](https://www.cytiva.com/contact) から入手可能な連絡フォームをご使用ください。

## 2 プライバシーとセキュリティの環境

### 環境におけるプライバシーとセキュリティ

Sepax S-100, Sepax 2 RM, and Sepax C-Pro は、プライバシーとセキュリティの保護に関する以下の期待事項に従って、指定の用途に使用するように設計されています。これらの期待事項は Sepax S-100, Sepax 2 RM, and Sepax C-Pro の使用環境に導入すべきです。

- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、ネットワークモードと隔離モードの両方で稼働できます。Cytiva は、ネットワーク機能のない隔離された環境で使用することを推奨します。ネットワークモードでは、ネットワークに接続されたすべての機器のセキュリティを保護するために、ファイアウォールの保護が必要です。詳細は [セクション 5.2 有線ネットワークのセキュリティ](#)、[~ ページに 21](#) を参照してください。

**注釈:** ユーザーは、ネットワークインフラストラクチャの安全性を確認する責任があります。

- Cytiva は、オペレーティングシステム (OS) に由来するセキュリティリスクについて責任を負いません。この機器の OS は古いため、セキュリティアップデートやパッチは今後提供されません。詳細は [セクション 6.2 システム変更の管理](#)、[~ ページに 32](#) を参照してください。
- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器はユーザー名とパスワードを使ってユーザー名とパスワードで保護されています。認証コントロールと承認コントロールの両方が実装されています。
- Cytiva は、情報システムの認証に加えて、ローカルバッジやキーリーダーシステムなどの運用上の物理セキュリティを導入することを推奨しています。
- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、Windows のデフォルトのファイアウォールを有効にした状態で設定されています。
- モバイル機器としてではなく、据え置き型の卓上機器として使用することが推奨されます。
- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器のユーザーは、実験室の環境に関する知識を持ち、システムを操作するためのトレーニングを受けていることが必要です。
- 機器の修理は、訓練を受けた Cytiva 社員または Cytiva が認定した第三者が行う必要があります。
- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器はそれぞれ、*Sepax Cell Separation System Operator Manual (14801)*、*Sepax C-Pro Operating Instructions (29350570)*、および付属のアプリケーションのオペレーターマニュアルに従って操作する必要があります。

お客様は、関連する操作メカニズムを定義する責任を負い、使用方法に関する明確化について Cytiva に問い合わせることができます。Cytiva は、*Sepax Cell Separation System Operator Manual (14801)*、*Sepax C-Pro Operating Instructions (29350570)*、アプリケーションのオペレーターマニュアル、またはマーケティング資料に明示されている以外の、お客様が考案した使用のシナリオについて責任を負いません。

# 3 認証、認可、監査ログの取得

## 本章に関して

Sepax S-100, Sepax 2 RM, and Sepax C-Pro には、プライバシーとセキュリティを有効にするためのさまざまな機能が搭載されています。本章では、これらのプライバシー機能とセキュリティ機能の機能性と使用について説明します。

## 本章の構成

セクション		参照ページ
3.1	アクセスコントロール	8
3.2	監査ロギングとアカウントビリティコントロール	16

## 3.1 アクセスコントロール

### はじめに

Sepax S-100, Sepax 2 RM, and Sepax C-Pro のアクセスコントロールを使用して、システムの顧客情報へのアクセスをコントロールします。アクセスコントロールには、ユーザーアカウントの作成、特権の割り当てなどといった機能が含まれています。

このセクションでは、ユーザーの情報へのアクセスを制御するための情報を提供します。

### 本セクションの構成

セクション	参照ページ
3.1.1 ID のプロビジョニング	9
3.1.2 パスワード	11
3.1.3 ユーザー認証	12
3.1.4 アクセス権の割り当て	13



## 3.1.1 IDのプロビジョニング

### はじめに

ユーザーアカウントのプロビジョニングには、アカウントの作成手順、メンテナンス手順、アカウントが不要になった際のアカウントの削除手順が必要です。ユーザーアカウントは特定の個人による使用を目的として作成されます。このユーザーアカウントは、アクセス権に関連しており、システムログファイルに記録されます。

**注釈:** この情報システムには、ユーザーの**First name**(姓)、**Middle name**(ミドルネーム)、**Last name**(名)が保存されます。Cytiva は他のいかなる目的にもこの情報を使用することはありません。ユーザーアカウントの情報の提供はお客様ご自身の判断で行ってください。個人のプライバシーを尊重すると同時に、ユーザーをアカウントと個別に照合する必要性も尊重すべきです。

### ユーザーアカウント

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器に搭載されているソフトウェアは、以下の役割を持つユーザーアカウントを認識します。

役割	説明
<b>事前定義済みアカウント</b>	
<b>ADMIN</b> (管理)	サービスメニューを除くすべての機能にアクセスできる管理者アカウント。 このアカウントは、 <b>管理者</b> ユーザーが作成 / 変更できます。
<b>SERVICE</b> (サービス)	サービスエンジニア向けのサービスアカウントです。 このアカウントでは、お客様は変更はできません。
<b>顧客定義済みアカウント</b>	
<b>User</b> (ユーザー)	あらかじめ設定されたパラメータでアプリケーションを実行できる基本的なユーザーアカウントです。 このアカウントは、 <b>管理者</b> ユーザーが作成 / 変更できます。

### ローカルユーザーのユーザーアカウント管理

お客様で個別にユーザーアカウントを作成していただく必要があります。ユーザーアカウントを管理する際には、以下の点を考慮してください。

- 管理者は、ユーザーアカウントを作成できます。
- 管理者は、ユーザー名、パスワード、アカウント権限など、ユーザーアカウントの詳細を管理できます。
- 管理者は、ユーザーアカウントを有効化または一時停止できます。

### 3 認証、認可、監査ログの取得

#### 3.1 アクセスコントロール

##### 3.1.1 IDのプロビジョニング

- 管理者はユーザーアカウントを完全に削除することができます。その結果、データベースからすべてのユーザーデータおよびユーザー参照が削除されます。

**注釈:** 本情報システムは非アクティブユーザーの自動削除に対応していません。管理者による無効化は、手動で行う必要があります。

- ユーザーアカウントの削除または無効化に関連するすべてのイベントは、監査目的のためにログファイルに記録されます。
- システムは常に1つのデフォルトの **ADMIN** アカウントを保持し、その役割に関係なく、どのユーザーも削除できません。
- 管理者がシステムにアクセスできなくなった場合、サービス担当者は管理者パスワードをリセットできます。

## 3.1.2 パスワード

### パスワードの変更

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器はデフォルトの管理者アカウントで提供されますが、初回使用時にパスワードの再設定が必要です。

管理者ユーザーは、アカウントの作成時に、新たに作成したユーザーの仮パスワードを登録します。Cytiva はユーザーが最初のログイン時に仮パスワードをリセットすることを推奨します。

### パスワードの要件

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器にローカルモードでログインする場合は、次のパスワード要件が適用されます。

- パスワードは最低6文字でなければなりません。
- パスワードには、以下の3つのすべてのカテゴリが含まれていなければなりません。
  - 英文字 (A ~ Z)
  - !, \$, #, % など、アルファベット以外の文字
  - 数字 (0 ~ 9)

パスワードポリシー設定は固定されているため、再設定することはできません。

### 3.1.3 ユーザー認証

ユーザー認証の手続きにより、システムにアクセスしようとしているユーザーが、指定アカウントに関連付けられているユーザーであることを確認します。本項では、認証システムの管理について説明します。

- また、Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、ユーザー名とパスワードによるローカルユーザー認証に対応しており、スタンドアローンの機器として動作させることが可能です。
- Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器には、サービス利用者がサービスメニューにアクセスするために使用する特別な認証メカニズムがあります。
- 本情報システムでは、Windows オペレーティングシステムにアクセスするための Microsoft Windows 認証を内部で管理しています。
- パスワードなどの機密情報は、業界標準のハッシュアルゴリズムを用いて安全に保管され、セキュリティと完全性を確保します。
- すべてのユーザーアカウントのパスワードは、パスワードポリシーに従う必要があります。詳細については [セクション3.1.2 パスワード、~ページに11](#)を参照してください。
- ユーザーが **Max login attempts** ( デフォルト = 3 回 ) で設定した回数以上、間違ったパスワードの組み合わせを入力した場合、ログオンアカウントは無効化されます。管理者ユーザーはパスワードを再設定し、アカウントを有効にする必要があります。
- ユーザーフィールド ( **User ID**、**First name**、**Middle name** および **Last name** ) は、15 文字までとなります。

## 3.1.4 アクセス権の割り当て

### 説明

アクセス権の割り当ては、ユーザーアカウントに許可を結びつけるための管理プロセスです。

### 役割ベースのアクセスコントロール

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は 3 つのユーザーの役割に対応しています。

- **User** (ユーザー) (研究所のユーザー)
- **Administrator** (管理者) (研究所の管理者)
- **Service** (サービス) ユーザー (Cytiva Cytiva の許可を得ている要員または第三者)

**Administrator** (管理者) ユーザーと **Service** (サービス) ユーザーは、ユーザーの権限を割り当てることができます。**Service** (サービス) ユーザーは、すべての機能にアクセスすることができます。

### 許可されたユーザーアクション

以下の表は、ユーザーの役割に応じた利用可能なアクションを示したものです。定義については [セクション 3.1.1 ID のプロビジョニング](#)、[~ ページに 9](#) を参照してください。

アクション	User (ユーザー)	Administrator (管理者)	Service (サービス)
<b>操作</b>			
シャットダウン	✓	✓	✓
ログアウト	✓	✓	✓
アプリケーションの選択、実行、および停止	✓	✓	✓
アプリケーションのすべてのパラメータおよびトレーサビリティの表示、選択、使用	✓	✓	✓
アプリケーションのインストール	✓	✓	✓
<b>情報関連</b> の表示	✓	✓	✓
保護パラメータの編集	✗	✓	✓
強制入力 ID	✗	✓	✓
ISBT 128 のみ	✗	✓	✓

### 3 認証、認可、監査ログの取得

#### 3.1 アクセスコントロール

##### 3.1.4 アクセス権の割り当て

アクション	User(ユーザー)	Administrator(管理者)	Service(サービス)
トレースIDの有効化	✗	✓	✓
ユーザーデータの削除	✗	✓	✓
<b>ユーザー管理</b>			
ユーザーの作成、編集、削除	✗	✓	✓
ユーザー役割の修正	✗	✓	✓
ユーザーのパスワードのリセット	✗	✓	✓
ユーザーのステータスの修正 (アクティブまたは一時停止)	✗	✓	✓
ユーザーのパスワードをリセットします。	✓	✓	✓
<b>データファイル</b>			
サマリーファイルの保存/送信	✓	✓	✓
システムログを含むログファイルの保存	✓	✓	✓
サポートファイルの保存	✓	✓	✓
レポートファイルの保存、表示、および印刷	✓	✓	✓
構成レポートファイルの保存、表示、および印刷	✓	✓	✓
<b>パッケージマネージャ</b>			
インストールしたアプリケーションの表示	✓	✓	✓
アプリケーションのインストールとアンインストール	✗	✓	✓
アプリケーションの有効化と無効化	✗	✗	✓
GMAP 更新のインストール	✗	✓	✓
<b>設定</b>			
音量と輝度の設定	✓	✓	✓
日時の設定	✗	✓	✓
言語の設定	✗	✓	✓
<b>自動印刷</b> データの設定	✗	✓	✓

### 3 認証、認可、監査ログの取得

#### 3.1 アクセスコントロール

##### 3.1.4 アクセス権の割り当て

アクション	User(ユーザー)	Administrator(管理者)	Service(サービス)
ファイル名ドネーションID	✗	✓	✓
自動ログオフの有効化	✗	✓	✓
無活動タイムアウト	✗	✓	✓
ログイン試行回数の上限	✗	✓	✓

アクション	Service only(サービスのみ)
<b>Service</b> (サービス) メニューの表示と使用	✓
メンテナンス/アプリケーションテストの実行	✓
アプリケーションのアクティベーション	✓
シリアル番号の設定	✓
SepaxNet 設定の編集	✓
モニターハードウェア	✓
ハードウェアの較正	✓
専用設定の編集	✓
ハードウェアの設定	✓
ユーザーデータの削除	✓
システムの詳細情報の表示	✓

## 3.2 監査ロギングとアカウントビリティコントロール

### はじめに

プライバシーとセキュリティに関する情報の記録と管理は、セキュリティ監視、監査可能な記録、および報告を通じて説明責任を果たします。

### ローカルログファイル

以下のログファイルが保存され、システムからエクスポートできます。

- サマリーファイル:
- システムログ
- ログファイル:
- レポートファイル:
- サポートファイル:
- 設定レポート

### ログファイルの内容

各ファイルタイプの内容は、以下の表のとおりです。

ファイルのタイプ	説明
サマリー	手順とトレーサビリティ情報、およびすべてのアプリケーションパラメータ、異なるアクションからのステータス情報、手順、および同様のものを含むカスタム拡張機能ベースのテキストファイルです。
システムログ	システム上で行われたアクションをカテゴリ別に記録したファイル <sup>1</sup> 操作を行ったユーザーのID、各操作のタイムスタンプを参照してください。
ログ	全センサーから収集したあらゆる詳細データが保存されているCSV (カンマ区切り) ファイルです。
レポート	実行されたプロシージャのカスタム PDF レポートファイルで、サマリーファイルから作成されます。
サポート	すべての詳細ログ、サマリーおよびレポートファイル、トレーサ情報を含む圧縮ファイル (データベースおよび設定情報を含む場合もあります)。このファイルはカスタムパスワードで保護されており、エラーや前例のないシナリオを報告するために製品チームに送信できます。



### 3 認証、認可、監査ログの取得

#### 3.2 監査ロギングとアカウントビリティコントロール

ファイルのタイプ	説明
設定レポート	機器設定のスナップショットや、インストールされているアプリケーションのリストを含むPDFファイルです。

<sup>1</sup> システムログのカテゴリの詳細については *Sepax Cell Separation System Operator Manual (14801)* または *Sepax C-Pro Operating Instructions (29350570)*、

## 4 被検者プライバシー同意の管理

### 被検者プライバシー

被検者プライバシー同意の管理は、被検者のプライバシー要件に関して被検者を支援するプロセスです。これは他の形式の同意（治療に対する同意など）とは異なります。

Sepax S-100, Sepax 2 RM, and Sepax C-Pro は、患者データを取り扱わない（作成、転送、保存しない）ため、患者プライバシー同意書は Sepax S-100, Sepax 2 RM, and Sepax C-Pro に適用されません。

ドナー ID を入力欄に使用する場合は、ユーザーはドナー ID が匿名化されていることを確認する必要があります。本情報システムでは、入力に基づいた入力フィールドの識別や処理は行われません。

さらに、サポートおよびエラー診断を容易にするために、機密情報（例えば、ドナー ID、**User Id**（ユーザー（ユーザー ID）、**First name**（名）、**Middle name**（ミドルネーム）、**Last name**（姓））を Cytiva が収集する場合があります。Cytiva は不測の情報開示に対して一切責任を負いません。いかなる方法によっても Cytiva がこの情報を使用することはありません。お客様は、データの安全性を確保するために、例外的に、各社のプライバシーポリシーに従った措置を講じる必要があります。

# 5 情報の保護

## 本章に関して

本章では、プライバシーとセキュリティに関する処理を説明します。Sepax S-100, Sepax 2 RM, and Sepax C-Pro の安全な環境の準備に関するガイドラインも含まれています。

## 多重防護

総合的な「多重防護」情報保証戦略の一環としてセキュリティ処理がしっかりと実装されています。この戦略は、人材、物理的セキュリティ、テクノロジーに対応する情報技術システム全体にわたって使用されます。多重防護の断層化アプローチにより、1つのセキュリティ対策の失敗によりシステムのセキュリティ侵害を許してしまうリスクを制限します。

## 本章の構成

セクション	参照ページ
5.1      キオスクモード	20
5.2      有線ネットワークのセキュリティ	21
5.3      無線ネットワークのセキュリティ	22
5.4      リムーバブルメディアのセキュリティ	23
5.5      保存データのセキュリティ	25
5.6      バックアップに関する注意事項	26
5.7      データ完全性	27
5.8      データ保持ポリシー	28
5.9      データ破壊ポリシー	29

## 5.1 キオスクモード

### はじめに

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、システムソフトウェアがあらかじめインストールされた完成品として出荷されます。システムはキオスクモードで構成されており、ソフトウェアやオペレーティングシステムの変更は、Cytiva 社員または Cytiva が認定した第三者が行う必要があります。

### キオスクモード機能

キオスクはソフトウェアの制限です。システムの電源を入れると、ユーザーはシステムソフトウェアインターフェースにのみアクセスできます。キオスクモードでは、オペレーティングシステムと管理機能にアクセスできません。

ソフトウェアまたはオペレーティングシステムの機能および設定の変更は、Cytiva 社員または Cytiva が認定した第三者のみが行うことができます。サービス担当者は、制限された環境を出て、Windows の機能にアクセスするために、別の認証メカニズムを使用します。

## 5.2 有線ネットワークのセキュリティ

### はじめに

Cytiva は、GMAPv5.5.x のソフトウェアバージョンを持つ医療情報システムをネットワークに接続しないことを推奨しています。どうしてもネットワークに接続しなければならない場合は、医療情報システムを不正侵入から保護された安全なネットワーク環境で運用することを強く推奨します。ファイアウォール保護、非武装地帯 (DMZ)、仮想ローカルエリアネットワーク (VLAN)、ネットワークエンクレープなど、医療情報システムの隔離と保護のための効果的な技術が多数存在します。

安全なネットワーク設計に役立つように、以下のセクションに Sepax S-100, Sepax 2 RM, and Sepax C-Pro の必須ネットワークサービスの概要が示されます。

### ネットワークのセットアップ

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器が節電モードに入っています。ネットワーク関連の設定は、Cytiva の社員または Cytiva が認定した第三者が行う必要があります。

### ファイアウォール

Windows ファイアウォールはすべてのネットワークのエンドポイントに対して有効になっており、設定されています。

### データ履歴への節儉

Sepax S-100, Sepax 2 RM, and Sepax C-Pro は、結果データファイルを保存するために、サポートされているデータ履歴機器 (SepaxNet) にオプションで接続します。

ローカルネットワークモードで接続された SepaxNet は非セキュアですが、後方互換性の理由からまだサポートされています。Cytiva では、セキュリティ上の理由から SepaxNet 機器の使用を推奨していません。エンドユーザーは、SepaxNet をワークフローに組み込む前に、自己責任でデューデリジェンスすることをお勧めします。Cytiva は、SepaxNet の接続により生じるデータのセキュリティまたはプライバシーに関するリスクについては一切責任を負いません。

### リモートサービスとセキュリティ

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、同梱の TeamViewer アプリケーションを使用してリモートサービスを行うことができます。すべてのサービス利用者は、リモートサービスにアクセスするための特別なパスワードを持っています。詳細については [第7章 リモートアクセス、~ ページに 33](#) を参照してください。

TeamViewer の接続プロトコルは、リモート接続のためのセキュリティに配慮しています。

## 5.3 無線ネットワークのセキュリティ

### 無線通信

無線ネットワーク通信では無線信号が使用されるため、無線機器には特別なセキュリティ配慮が必要です。無線通信のセキュリティを向上させるために、有効な技術やツールが存在します。このセクションでは、Sepax S-100, Sepax 2 RM, and Sepax C-Pro の無線接続に関する特性を説明します。

### 無線ネットワーク接続

Cytiva は、Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器で有線ネットワークの代用として無線ネットワーク機能を使用することを推奨しません。ただし、Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は無線機能に対応はしています。

Cytiva 社員または Cytiva 認定の第三者が、Sepax S-100, Sepax 2 RM, and Sepax C-Pro の無線ネットワークを設定する必要があります。

Sepax S-100, Sepax 2 RM, and Sepax C-Pro の各機器は、以下の場合に無線接続を使用できます。

- データアーカイブのためにデータ履歴との接続を行う場合
- リモートサービスセッション中に無線ネットワークの施設に接続する場合

外部アクセスポイントや USB Wi-Fi ドングルで無線接続する場合、最低限以下のセキュリティ設定をすることをお勧めします。

- WPA2
- AES
- パスワード：固定静的パスワード

## 5.4 リムーバブルメディアのセキュリティ

### はじめに

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器では、5 つの USB ポートと 2 つの Ethernet ポートを使用して、リムーバブルメディアやデバイスからデータをインポートおよびエクスポートすることが可能です。

以下のセクションでは、データの完全性と安全性のために実施されたセキュリティ対策について説明します。

### リムーバブルメディア

ユーザーには、システムに接続される取り外し可能なデバイスをウイルスやその他のマルウェアに感染させないようにする責任があります。

**注釈:** Cytiva は、Cytiva が支給する USB フラッシュドライブのみを使用することをお勧めします。支給された USB フラッシュドライブは Sepax S-100 機器以外のいかなる用途にも使用しないでください。

本製品には、以下の USB フラッシュドライブが付属しています。

USB フラッシュドライブのタイプ	説明
データ用の USB フラッシュドライブ	フラッシュドライブには次の 2 つのパーティションが含まれます。 <ul style="list-style-type: none"> <li>データ保存用のパーティションを 1 つ用意。</li> <li>ユーザードキュメント用にパーティションを 1 つ用意。</li> </ul>
アプリケーションインストール用の USB フラッシュドライブ	アプリケーションのインストーラーが入ったフラッシュドライブ。

### ファイルアクセスおよび制限

USB フラッシュドライブのファイルシステムには、アプリケーションソフトウェアからのみアクセス可能です。

Sepax S-100, Sepax 2 RM, and Sepax C-Pro からレポートやログファイルを USB フラッシュドライブにエクスポートできます。USB フラッシュドライブからインストールできるのは、アプリケーションのみです。

### AutoPlay の無効化

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器では、自動再生（古い OS では AutoRun と呼ばれる）と USB フラッシュドライブからの実行権が無効化されます。

## 付加的なセキュリティ対策

USB フラッシュドライブでアプリケーションの実行権限を無効化しました。



## 5.5 保存データのセキュリティ

### はじめに

保存されているデータのセキュリティを確保するために、以下のセキュリティ対策が講じられています。

### データストレージ

ユーザー情報と機器情報は、データベース記録の一部またはアプリケーションログの一部として保存されます、暗号化はされません。Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、ローカルユーザーに関する以下の情報を保存します。

- 名称
- ID (固有のユーザー ID)
- パスワード
- 役割 ( アクセスレベル )

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器には、以下のような情報が保存されています。

- IP アドレス
- ホスト名
- 現在のオペレーティングシステム
- 本装置のセンサー情報

Cytiva は不測の情報開示に対して一切責任を負いません。Cytiva は、保存された情報を一切使用しません。お客様は、例外的に、ご自身の個人情報保護方針に従って、データの安全性について適切な措置を講じる必要があります。

### パーティションの完全性

オペレーティングシステムは、以下の2つのパーティションに分かれています。

- システムパーティション
- データパーティション

システムパーティションは書き込みフィルターによって保護されており、システムの電源を入れるたびに、オペレーティングシステムと対応するアプリケーションソフトウェアのファイルが元の状態にあることを確認します。

データパーティションの整合性は、以下の対策により保護されています。

- システムはキオスクモードで動作します、詳しくは [セクション5.1 キオスクモード、~ページに20](#) をご覧ください。
- ユーザー認証情報は、ソルトとハッシュが付けられた上でデータベースにローカルで保存されます。

## 5.6 バックアップに関する注意事項

### Delete user data

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、**ユーザーデータの削除機能**を使用して、製造時の初期設定に戻すことができます。



#### 注記

すべてのシステムデータ（手続きデータファイルやシステム設定など）が削除されます。この手続きは、管理者またはサービスユーザーが行う必要があります。確認後は、最新のバックアップ状態での復元のみ可能です。

### Backup

**バックアップ機能**により、システムデータ（アプリケーション、手順データファイル、システム構成など）のバックアップを作成し、機器に接続されたUSBフラッシュドライブに保存することができます。バックアップのたびに新しいファイルが作成され、保存されます。

## 5.7 データ完全性

### データ完全性機能

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器には、データが偶発的または悪意を持って不適切に変更されないようにするための機能が含まれています。

- 実行ファイルと DLL は、データの整合性を保つために保護されています。
- 本アプリケーションシステムへの入力はずべて、入力検証を通じて検証されます。
- 入力ファイル ( xml ファイルなど ) はすべて、本情報システムによって使用される前に検証されます。
- ユーザー管理には、セキュアなパスワードが設定された内部データベースを使用します。
- バックアップ用の zip ファイルは、動的に生成されるパスワードで保護されています。

### 非特定化機能

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は患者データを扱わない ( 作成、転送、保存 ) ため、非識別化 ( 匿名化および仮名化 ) 機能は含まれていません。

ユーザーは Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器で使用する前に、サンプル処理で使用するサンプル ID を匿名化する必要があります。

### ビジネス継続性

ビジネスの継続性を確保するために以下の対策を講じます。

- OS やアプリケーションソフトウェアのデータが破損した場合、システムの電源を入れるとファイルが元の状態に戻ります。
- 停電時には、記憶媒体が遅延書き込みを行い、データを保存します。
- 本システムは、高い再訪回復力を確保し、細胞喪失を最小限に抑えるために、アプリケーション障害発生時の細胞回復手順に対応しています。

### クラウドプロバイダにより提供されるセキュリティコントロール

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、クラウド機能や配信データアーキテクチャを利用しません。データはすべてローカルで保存し、オプションとして SepaxNet に集約させることもできます。

## 5.8 データ保持ポリシー

Sepax S-100, Sepax 2 RM, and Sepax C-Pro は、長期間の記録保持やアーカイブ用に設計されていませんが、対応するデータ履歴プラットフォームへの正確で完全なエクスポートや、一般的なポータブルフォーマットでの安全で保護されたファイルのエクスポートが可能です。

ユーザーは、記録およびデータ保持ポリシーを満たすために、適切な手配がなされていることを確認する必要があります。システム本体に保存できるサマリーファイル、レポートファイル、センサーデータファイルの数には制限があります。Sepax S-100, Sepax 2 RM, and Sepax C-Pro システムは、*Sepax Cell Separation System Operator Manual (14801)*、*Sepax C-Pro Operating Instructions (29350570)*、およびアプリケーションのオペレーターマニュアルに記載されているように動作するためのアプリケーションデータ、ユーザーデータ、設定データを保存します。

ログファイルは 32 個のレコード、サマリーファイルは 50 個のレコードまでという記憶容量の制限があります。システムログは最大 1 年間保存されますが、より長期間の保存が必要な場合は、エクスポートする必要があります。システム構成によっては、情報をデータ履歴（例：SepaxNet）にエクスポートしたり、*Sepax Cell Separation System Operator Manual (14801)* および *Sepax C-Pro Operating Instructions (29350570)* に定義されているように手動でエクスポートしたりすることができます。

システム管理者は、すべてのユーザー、ユーザーが生成したデータ、アプリケーションの設定の削除、管理者パスワードのデフォルトへのリセットを含む、ユーザーデータの削除を行うことができます。また、サービスエンジニアだけが利用できるバックアップ機能も備えており、すべてのデータを二次記憶装置にバックアップすることが可能です。本機に保存されているすべての記録とログは、認定されたフィールドサービスエンジニアのみが適用できるファクトリーリセットによって削除できます。

## 5.9 データ破壊ポリシー

本システムから収集されたデータがシステム診断とエラー調査以外の目的で使用されることはありません。二次ストレージにローカルで保存されているデータはすべて、お客様のデータ保護ポリシーにより管理されます。例外的な状況、例えば二次記憶装置の故障などでは、お客様はデータのプライバシーと機密保持に責任を負います。

情報システムで取得したデータは、1年間限定で保存されます。システムの記憶容量は、[セクション5.8 データ保持ポリシー](#)、[~ページに28](#)に記載されています。Cytivaでは、二次ストレージメディアの物理的衝突が発生した場合、そのメディアを廃棄する前に、Gutmann方式（35パス）のデータ消去またはこれに相当する戦略を実施することを推奨しています。

## 6 システムの保護

### はじめに

本章では、プライバシーとセキュリティを継続的に保護できる方法を用いた本製品の設定方法とメンテナンス方法のガイドラインについて説明します。

### 本章の構成

セクション	参照ページ
6.1 悪質なソフトウェアからの保護	31
6.2 システム変更の管理	32

## 6.1 悪質なソフトウェアからの保護

### 悪質なソフトウェア

コンピュータ環境はますます厳しくなり、サービス妨害攻撃やコンピュータウイルス、ワーム、トロイの木馬などの悪質なソフトウェアによる脅威が増え続けています。悪意のあるソフトウェアに侵入されないようにするためには、さまざまなレベルで精力的に防御することが必要です。多くの場合、効果的な保護には、Cytivaと当社のお客様の協力が必要です。

### 悪意のある攻撃からの保護

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、ウイルスやマルウェアの感染リスクを低減するキオスクモードで動作し、システム上でWindows ファイアウォールが有効になっています。しかし、ウイルス対策 / マルウェア対策はいずれも統合 / 有効化されておらず、サードパーティ製のウイルス対策ソフトウェアのインストールに関する技術サポートも提供されていません。

ユーザーの責任で以下を確認する必要があります。

- システムに接続されたリムーバブルデバイスは、ウイルスなどのマルウェアに感染していないこと。
- ネットワークモードで使用する場合、ネットワークインフラはファイアウォールなどのセキュリティ対策が施されています。

## 6.2 システム変更の管理

### はじめに

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器は、装置のハードウェアとシステムソフトウェアで構成され、すぐに使用できる状態で出荷されます。システムはオペレーティングシステムへの不正アクセスを防止するキオスクモードで動作します。

お客様が発見されたセキュリティリスクは、[cytiva.com/contact](https://cytiva.com/contact) にあるコンタクトフォームを使用して、Cytiva に報告する必要があります。

### ソフトウェアの更新

パッチやバージョンアップなど、システムまたはアプリケーションソフトウェアのすべての変更は、Cytiva によって管理されます。オペレーティングシステムやアプリケーションソフトウェアのアップグレード、メンテナンス、変更は、Cytiva 社員または Cytiva が認定した第三者のみが特別な認証機構を使用して行うことができます。

Sepax S-100, Sepax 2 RM, and Sepax C-Pro は Windows XP Embedded Service Pack 3 で動作しますが、これは旧式であり Microsoft のサポートが終了しています。上記の OS に対してはセキュリティのアップデートやパッチは使用できなくなります。現在、Cytiva は、ネットワーク機能のない隔離された環境で Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器を使用することを推奨します。別の条件下で機器を使用する場合は、お客様ご自身の判断で行ってください。Cytiva は、オペレーティングシステムに由来するセキュリティリスクについて責任を負いません。



# 7 リモートアクセス

## はじめに

Cytiva によるサービス提供の最も効率的でコスト効果の高い方法とは多くの場合、Sepax S-100, Sepax 2 RM, and Sepax C-Pro へのリモート接続です。この接続を可能な限り安全なものにするために最大限の力が注がれています。この章では、リモートアクセス接続時のセキュリティ対策について説明します。

## リモートサービスソフトウェア

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器のリモートサービスには、リモートソフトウェアアップデート、診断、アップグレード、ソフトウェアパッチの配信が含まれます。Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器にはリモートモニタリング機能もリモート実行機能もありません。

Sepax S-100, Sepax 2 RM, and Sepax C-Pro 機器のリモートサービスは、サードパーティ製ソフトウェア TeamViewer を使用して、Cytiva 社員または Cytiva によって認定を受けた第三者によってのみ実行できます。

TeamViewer は Sepax S-100 機器にプリインストールされており、以下の機能を提供します。

- 中央認証
- 機械匿名化
- 活動ログ
- ユーザーアクセスコントロール
- 安全なファイル送信
- 暗号化されたリモート接続

現在、Cytiva リモートサービスセッション用の活動追跡機能はありません。しかし、Cytiva のリモートサービスにはユーザーからの確認が必要です。

## 8 本製品により収集された個人情報

### 個人情報

本情報システムでは、被検者の個人情報の収集や保存は一切行われません。パスワードやユーザー名、**User ID**（ユーザーID）、**First name**（名）、**Middle name**（ミドルネーム）、**Last name**（名）などの機密情報は、業界標準のハッシュアルゴリズムを用いて安全に保管され、安全性と完全性を保証しています。

### その他の情報

システムが保存している情報の詳細は、[セクション5.5 保存データのセキュリティ](#)、[～ページに25](#)に記載されています。ドナーID番号に関するユーザーの責任については、[被検者プライバシー](#)、[～ページに18](#)をご覧ください。

## 9 製品セキュリティ補足資料

### 医療機器セキュリティのための製造 者開示説明書 ( MDS2 )

MDS2 は、ご要望に応じて、Sepax S-100 および Sepax 2 RM に利用できます。  
営業担当者にお問い合わせいただくか、[cytiva.com/contact](https://cytiva.com/contact) から入手可能な連絡  
フォームをご使用ください。



## cytiva.com

Cytiva および Drop ロゴは、Life Sciences IP Holdings Corp. または Cytiva として事業を展開している関連会社の商標です。  
Sepax は、Global Life Sciences Solutions USA LLC の商標、または Cytiva として事業を展開している関連会社の商標です。  
Microsoft および Windows は、Microsoft group of companies の商標です。  
他のすべての第三者商標は各所有者の所有物です。

© 2020-2022 Cytiva

各地の営業所の連絡先については、以下を参照してください。 [cytiva.com/contact](https://cytiva.com/contact)

29494414 AD V:6 01/2023