電子カルテ導入における
オンプレミス vs クラウド

安全性・運用負荷・BCP（事業継続計画）の多角的な徹底比較

医療情報セキュリティの現状と課題

「3省2ガイドライン」改定とランサムウェア攻撃などのサイバー脅威急増に伴い、医療機関にはより強固で柔軟なセキュリティ対策が求められています。

「3省2ガイドライン」とは、厚生労働省・経済産業省・総務省の3省が策定した、医療情報を取り扱うシステムや事業者の安全管理基準の総称です。病院や診療所向けの厚労省ガイドラインと、ベンダー向けの経済産業省・総務省ガイドラインで構成されます。

2つの設置形態の基本概念

オンプレミス型（院内完結）

院内に専用のサーバー機器を設置し、閉域ネットワーク（院内LAN）のみで運用する形態。

特徴: データが院外に出ない安心感がある一方、物理的・技術的セキュリティ管理、バックアップ、保守対応のすべてを自院で負担します。

クラウド型（外部利用）

高度なセキュリティ基準を満たした外部データセンターのサーバーをネットワーク経由で利用する形態。

特徴: 専門家による24時間監視と自動アップデートが提供され、自院の運用負荷を大幅に軽減可能です。

物理的・設備セキュリティの比較

- **院内サーバー室の物理的限界:** 施鍵管理や防犯・耐震設備、空調管理を自院で万全に保つには高額な費用が発生します。
- **専門データセンターの堅牢性:** クラウド基盤は24時間365日の有人監視、生体認証アクセス、自家発電装置を完備しています。
- **自然災害への耐性:** 地震・水害・停電発生時でも、データセンター側の redundancy（冗長化）によりシステム停止を防ぎます。



セキュリティ評価の3大要件

機密性 (Confidentiality)

不正アクセスや情報漏洩を防止。厳格なアクセス権限制御、多要素認証（MFA）、通信および保存データの暗号化を実施。

完全性 (Integrity)

改ざんや破壊からデータを保護。操作ログの改ざん不可保管、定期的な整合性検証と自動バックアップ体制の確立。

可用性 (Availability)

必要な時にいつでも電子カルテが利用可能。障害・災害時のBCP対策、高稼働率（SLA99.9%以上）の維持。

主要なセキュリティ項目一覧比較

比較項目	オンプレミス型		クラウド型	
物理的セキュリティ	自院責任 鍵管理・空調に限界あり	自院責任	極めて高い 専門DCで24時間監視	極めて高い
サイバー攻撃対策	遅れがち 手動での各種パッチ適用	遅れがち	常に最新 自動で最新定義を反映	常に最新
BCP・災害対策	高負担 自前での遠隔バックアップが必要	高負担	標準装備 地理的分散バックアップ	標準装備
責任範囲	自院がすべての安全管理責任を負う		事業者との「責任分界点」を明確化	

災害発生時の復旧性（BCP）の差

99.9%

サービス稼働率（SLA）保証

迅速な復旧とデータ損失の最小化

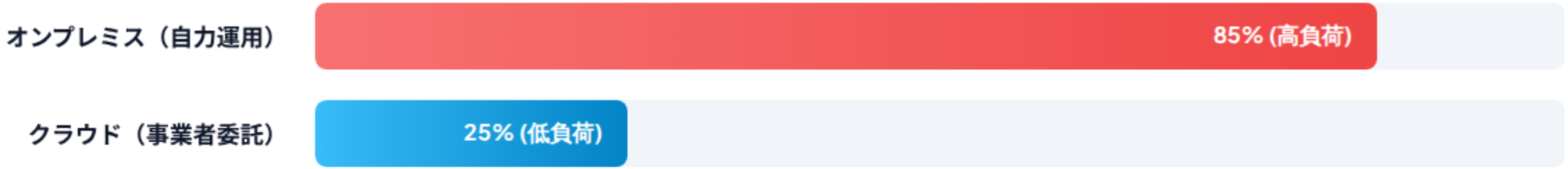
クラウド型電子カルテは、地理的に分散された複数のデータセンターへリアルタイムまたは高頻度でバックアップを同期しています。

万が一、病院が被災・停電した場合でも、予備端末やモバイル回線を用いて別の場所から即座にカルテ閲覧・入力業務を再開可能です。

3省2ガイドライン適合のポイント

- **責任分界点の明示（SLA・契約書）:** 医療機関とクラウド事業者間で、どこまでが誰の管理責任かをガイドラインに基づき明確に規定する。
- **安全なネットワーク接続:** IP-VPNやIPsecなどの閉域網、あるいは端末認証・暗号化された高度な通信を用いてアクセス制限を実施する。
- **厳格なログ管理と監査追跡:** 「誰が・いつ・どの患者のカルテを閲覧・更新したか」のアクセスログを長期間安全に保管・追跡可能にする。
- **外部認証の獲得状況確認:** 事業者がISMS（ISO27001）やSOC2レポート、3省2ガイドライン準拠チェックリストを開示しているか確認する。

セキュリティ運用における院内負担感



オンプレミスではOS更新・ウイルス対策・バックアップ確認などを院内IT担当者が行う必要がありますが、クラウドではその大部分を事業者が代行するため、日常のセキュリティ運用コストを大幅に削減できます。

安全な導入・移行の4ステップ

STEP 1

現状分析・要件確認

3省2ガイドラインに基づく要求事項と自院要件の整理

STEP 2

事業者選定・SLA確認

責任分界点・暗号化方式・バックアップ体制の評価

STEP 3

ネットワーク・端末構築

VPN接続、端末認証、アクセス権限の厳格な設定

STEP 4

運用テスト・院内教育

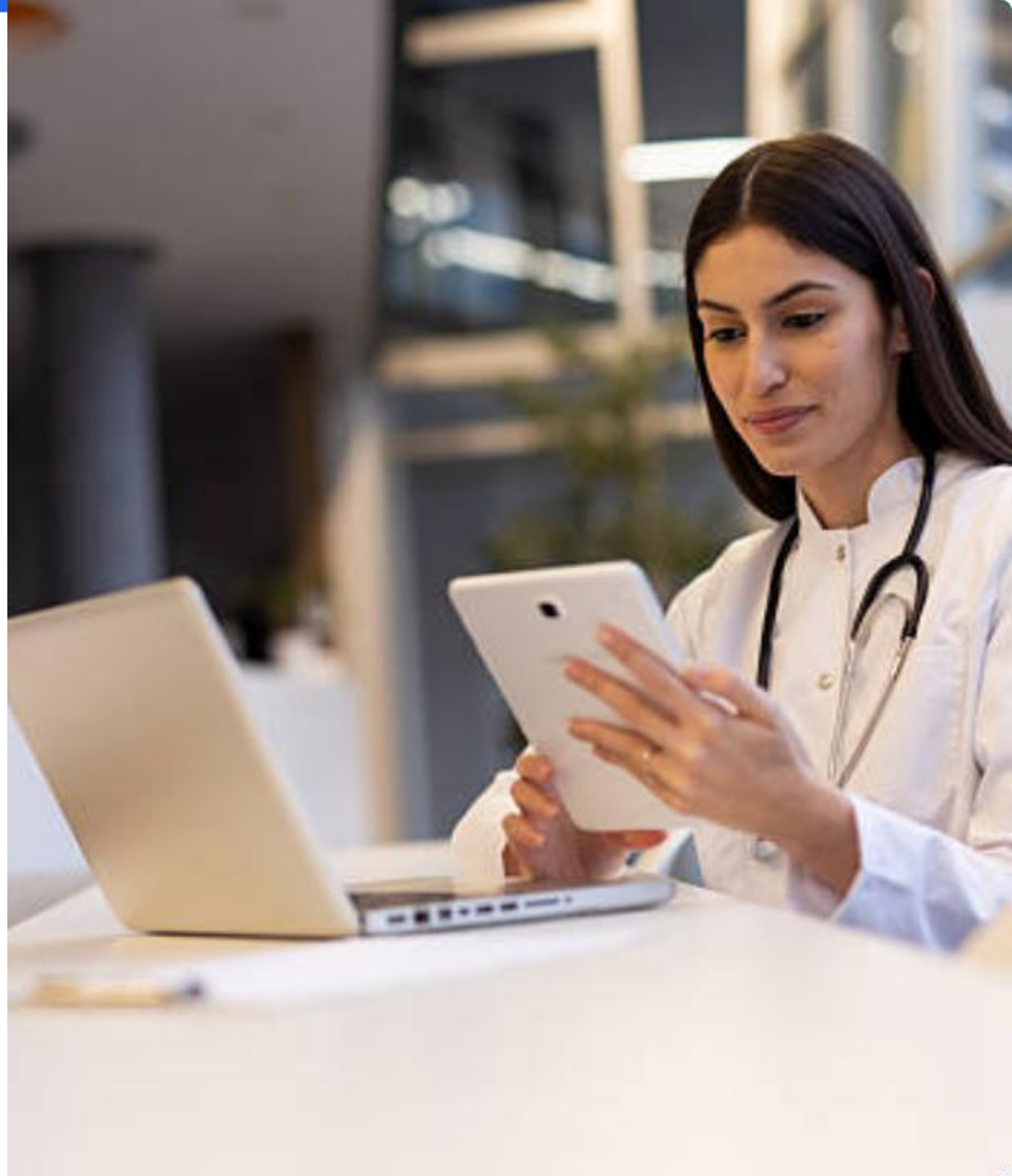
セキュリティポリシー徹底と非常時対応マニュアル制定

自院に最適なモデルの選択軸

システム選定の決定要因

院内に専任のIT管理者が存在し、特殊な部門システムや既存医療機器とのオンプレミス連携が必須な大規模病院では、従来型オンプレミスが選ばれるケースもあります。

一方で、IT人材の確保が難しく、災害対策（BCP）の強化や初期コスト抑制、最新セキュリティの自動享受を重視する多くのクリニック・中小病院では、クラウド型への移行が標準になりつつあります。



ご清聴ありがとうございました

電子カルテ導入・セキュリティ強化に関する質疑応答