情報区分	公開
発効日	2026/01/19
版番号	Ver.1.0

感情カルテ ホワイトペーパー

株式会社スカパー・カスタマーリレーションズ

〒141-0021 東京都品川区上大崎 3-1-1 JR 東急目黒ビル

改訂履歴表

版番号	発効年月日	改　訂　内　容
Ver.1.0	2026/01/19	新規制定

目次

はじめに

ホワイトペーパーの目的

株式会社スカパー・カスタマーリレーションズ（以下、「当社」という）は、
当社が提供する感情カルテ®で提供するサービス（以下「本サービス」という）
ご利用にあたり、本サービスの契約者「クラウドサービスカスタマ」（以下、「利用者」という）
へ提供する、ホワイトペーパー（以下、「本書」という）について記載します。

本書は、ISMS クラウドセキュリティ認証の要求事項「JIP-ISMS517-1.0（ISO/IEC27017）」により、クラウドサービスプロバイダが、クラウドサービスカスタマに向けて情報開示を求められている事項について、感情カルテにおけるセキュリティの取り組みを確認いただくことを目的としています。

クラウドサービスカスタマデータは、クラウドサービス上で保存、処理されます。クラウドサービス上のデータに対するセキュリティ対策は、主にクラウドサービスプロバイダによって担われることになります。ISO/IEC27017 では、クラウドサービスプロバイダは、クラウドサービスカスタマが、クラウドサービスにおける情報セキュリティ対策が、自身の情報セキュリティ要求事項を満たすかどうかを検証するために必要な情報を提供することが求められています。本書は、感情カルテのセキュリティの取り組みの理解の促進の一助になるべく策定されました。

なお、感情カルテの取り組みは、常に継続的に改善していきますので、最新の情報については、当社営業までご相談いただくか、当社 Web サイトをご確認ください。

【当社 Web サイト】
https://www.spcc-sp.com/compliance/

本書の適用範囲について

本書の適用範囲は、本サービス（以下、感情カルテ）となります。

本書で使用する用語について

本書で用いる用語及びその定義は、JIP-ISMS517-1.0、ISO/IEC 27017 および JIS Q 27017 によるものとします。また、これらの要求事項や規格で記されている用語については、改変せずに使用しております。

ISO/IEC 27017 とは

国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定する、情報セキュリティマネジメントに関する国際規格として、ISO/IEC 27000 シリーズがあります。その中で、情報セキュリティマネジメントシステムの要求事項である ISO/IEC27001 や、情報セキュリティ管理策の実践のための規範である ISO/IEC27002 は、組織が必要とする一般的な情報セキュリティについて規定されています。これらの規格に加えて、ISO/IEC27000 シリーズには、特定の分野固有の情報セキュリティ規格がいくつか策定されています。ISO/IEC27017 は、分野固有の情報セキュリティ規格の一つで、クラウドサービス特有のリスクに対応したクラウド分野固有の情報セキュリティ規格です。ISO/IEC27017 は、ISO/IEC27002 をベースとし、クラウドサービスプロバイダ及びクラウドサービスカスタマの双方に対して、クラウドサービスのための管理策及びクラウドサービスのための実施の手引を規定していることに特長があります。2016 年には、日本規格協会により、ISO/IEC27017 は、JIS Q 27017 として、JIS 化されています。

ISMS クラウドセキュリティ認証とは

ISMS クラウドセキュリティ認証とは、ISMS（ISO/IEC 27001）認証を前提として、クラウドサービスの情報セキュリティ規格（ISO/IEC 27017）を満たしている組織を認証する仕組みです。2016 年 8 月より一般財団法人日本情報経済社会推進協会（JIPDEC）により運用が開始されました。ISMS クラウドセキュリティ認証は、JIPDEC が定める「ISO/IEC 27017 に基づく ISMS クラウドセキュリティ認証に関する要求事項 JIP-ISMS517-1.0」を要求事項とし、ISMS アドオン認証と位置付けられています。

本サービスについて

感情カルテはパブリッククラウドに分類される SaaS（Softwear as a Service)のサービスです。

コンタクトセンターにて記録される通話録音データから、発話者の感情データを抽出、解析しコールセンターの円滑な運営に活用するためのレポート（感情カルテ）を提供するサービスになります。

本サービスのクラウド基盤にについて

感情カルテは、Amazon Web Service（以下、「AWS」という）の IaaS（Infrastructure as a Service）上で構築し本サービスを提供しています。

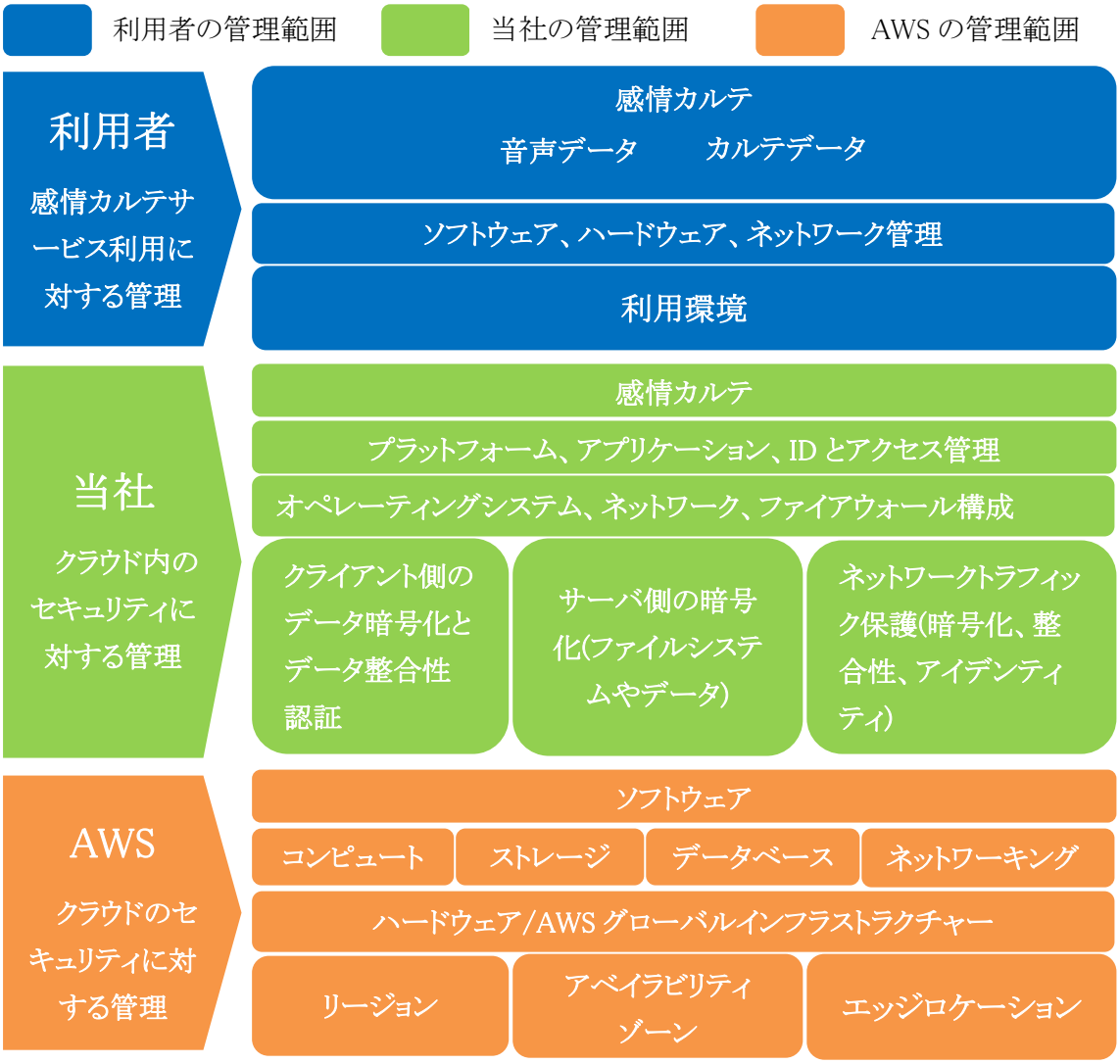
責任分界点について

本サービスに関する責任分界点は、以下のようになります。

■　本サービス 責任分界点

利用者 クラウドサービスカスタマ	当社 感情カルテ クラウドサービスプロバイダ	AWS クラウド基盤
入力・保管データの正確性・合法性、端末・ブラウザの衛生管理、接続元 GIP 管理、利用規約遵守	アプリ運用、アクセス制御、暗号化・バックアップ、監視・ログ管理、脆弱性対応、インシデント対応 メンテナンス及び通知、AWS 環境全般の管理運営	データセンター、ハードウェア、ネットワーク、ハイパーバイザー

■　本サービス 管理範囲



JIP-ISMS517-1.0、ISO/IEC 27017 への対応

JIP-ISMS517-1.0 への対応

4.1 クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001 の 4.3】

認証審査を受けるにあたって、組織は、クラウドサービスを含めた ISMS の適用範囲の決定を行い文書化することが求められています。当社においては、スコープを『本サービス』と定めています。

ISO/IEC 27017（JIS Q 27017）への対応

ISO/IEC 27017 は、ISO/IEC 27002 と共通する管理策については、同じ項番が付与されていますので、ISO/IEC 27001 附属書 A の項番とも一致します。

また、既存の ISO/IEC 27001 附属書 A および ISO/IEC 27002 で想定されていないクラウド特有の拡張された管理策については、「附属書 A（規定）クラウドサービス拡張管理策集」として、頭に『CLD』がつく項番が付与されています。また、頭に『CLD』がつく管理策についても、そのあとに続く番号は、ISO/IEC 27001 附属書 A および ISO/IEC 27002 で定められた番号とも整合がとられています。

本書においては、閲覧時の利便性を考慮し、項番の順番に沿って、クラウドサービスプロバイダとしての取り組みについて解説を行います。

5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダとして、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ方針の拡充が求められています。これらについては、当社の「クラウドセキュリティ基本方針」に従い、サービスを運用しています。また、「クラウドセキュリティ基本方針」は常に見直しを行い、クラウドサービスカスタマが安心して利用できるよう取り組んでいます。

6.1.1 情報セキュリティの役割及び責任

■当社の責任

有料サービスの提供

当社は、以下の義務を負うものとします。

1. 本サービス及び本コンテンツを、契約及び該当する注文書にしたがって利用者に提供すること。
2. 利用者に、有料サービスについて、追加料金なく、該当する当社の標準サポートを提供し、別途購入された場合には、アップグレードされたサポートを提供すること。
3. オンラインの有料サービスを、以下の場合を除き、1 日 24 時間、週 7 日提供する商業上合理的な努力を行うこと。
    - A) 計画停止（当社は、計画停止について、本ドキュメンテーションの定めにしたがって事前に電子的な通知を行うものとします）。
    - B) 当社の合理的管理を超える状況（例えば、不可抗力、政府機関の行為、洪水、火災、地震、暴動、テロ行為、ストライキその他の労働争議（当社の従業者による場合を除きます）、インターネ

ットサービスプロバイダの障害もしくは遅延、非アプリケーション又はサービス拒否（DoS）攻撃など）により生じた稼動停止。

当社要員

当社は、当社又は当社の関係会社の要員（従業者及び受託者を含みます）の本契約に基づく当社の義務の遵守につき責任を負うものとします。ただし、本契約に別段の定めがある場合には、この限りではありません。

■利用者の責任

利用者は、以下の義務を負います。

1. 本ユーザーの本契約、本ドキュメンテーション及び本注文書の遵守について責任を負うこと。
2. 本顧客データの正確性、品質、合法性、及び利用者が本顧客データを取得した方法について責任を負うこと。
3. 本サービス及び本コンテンツの不正アクセス又は不正利用を防止する商業上合理的な努力を行い、不正アクセス又は不正利用を発見したときには、速やかに当社に通知すること。
4. 本サービス及び本コンテンツを、本契約、本注文書、本ドキュメンテーション並びに適用ある法令及び政府規制にしたがってのみ利用すること。
5. 利用者が本サービス又は本コンテンツと共に利用する非アプリケーションのサービス条件を遵守すること。

6.1.3 関係当局との連絡

利用者のデータはすべて、日本にあるクラウドサービスのデータセンターに保管されています。

本サービス基盤	AWS（日本にあるデータセンター）

CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の分担

■利用者の責任範囲

1. 本サービス利用における管理責任
   - ・契約内容、利用規約、サービス仕様書の遵守
   - ・本サービスを通じて行われる利用者様の活動に関する管理
   - ・本サービスを通じて発信される情報の適切性の確保
   - ・第三者との間で生じた紛争等についての自己責任での解決
2. データ管理責任
   - ・データの内容：データの正確性、品質、適法性および取得方法についてはお客様の責任となります
   - ・バックアップ：当社は定期的なシステムバックアップを実施しますが、お客様の操作による誤削除等は復旧対象外となります
   - ・情報発信：本サービスを通じて発信される情報の内容についてはお客様が責任を負います
3. セキュリティ管理責任
   - ・アカウント管理：ユーザーアカウント、パスワード等の認証情報の厳格な管理
   - ・アクセス管理：適切な権限設定と接続元の管理

・端末セキュリティ：接続端末やブラウザのセキュリティ対策(ウイルス対策ソフトの導入等)
インシデント対応：不正アクセスや不正利用を発見された場合の速やかな当社への通

4. 利用環境管理責任
・本サービス仕様に定める動作要件を満たすクライアント環境(端末、ブラウザ、通信回線等)の準備と維持
・本サービスと連携する他のサービス等がある場合、それらのサービス条件の遵守

5. 法令遵守責任
・契約内容、利用規約、サービス仕様書の遵守
・関連法令および政府規制の遵守
・適法かつ適切な目的でのサービス利用

6. 損害賠償責任
・本上記責任範囲の不履行により当社が損害を蒙った場合の損害賠償
・本サービスの利用に関して第三者に対して損害を与えた場合の自己責任での賠償
・上記、定める事由より、当社が損害を蒙った場合には、利用者その損害を賠償するものとします。

■当社(クラウドサービスプロバイダ)の責任範囲

1. インフラストラクチャ管理責任
当社は、クラウド基盤上でのアプリケーション運用全般を管理し、適切なアクセス制御、データの暗号化およびバックアップを実施します。また、継続的な監視とログ管理により、セキュリティインシデントや脆弱性に迅速に対応いたします。

2. プラットフォーム・アプリケーション
システム基盤からアプリケーション層まで、包括的な管理責任を負います。これには、
オペレーティングシステムの適切な構成管理、最新のセキュリティパッチ適用
アプリケーションの開発・運用・保守が含まれます。

3. セキュリティ管理責任
本サービスにおける情報セキュリティ対策を実施し、以下の施策を講じています。
・データ暗号化: 通信経路および保管データの両方に対して、業界標準の暗号化技術を適用
・アクセス制御: 最小権限の原則に基づいた厳格なアクセス管理
・ログ管理: セキュリティ監査のための包括的なログ記録と適切な保存期間の設定
・バックアップ: 定期的なバックアップ実施とデータの安全な保管
当社の従業員および業務委託先に対しても、契約遵守とセキュリティ規程の徹底を図っています。・

4. データ保護責任
お客様の重要なデータを保護するため、以下を実施します。
・定期的な自動バックアップの実施
・システム障害時における迅速なデータ復旧
・契約終了時の安全かつ確実なデータ消去

5. 通知・開示責任
お客様への適時適切な情報提供を重視しています・

・計画停止に関する事前の電子的通知

・重大インシデント発生時の速やかな通知

・セキュリティ対策、サービス変更等の適切な情報開示

■AWS(クラウド基盤プロバイダ)の責任範囲

1. インフラストラクチャ管理

・データセンター:物理的セキュリティ、環境制御、電源、冷却

・ハードウェア: サーバー、ストレージ、ネットワーク機器の保守

・グローバルインフラ: リージョン、アベイラビリティゾーン、エッジロケーション

・物理ネットワーク: ネットワーク配線、ルーター、スイッチ

2. 仮想化・基盤サービス層

・デハイパーバイザー:仮想化基盤の管理と保護

・マネージドサービス:EC2 等のサービス基盤・

・基盤のパッチ管理:ハイパーバイザー、ホスト OS の脆弱性対応

・基盤の監視:AWS インフラの可用性監視

■ 責任の重複領域

1. セキュリティ(共同責任)

・利用者:認証情報管理、端末セキュリティ、データの適法な利用

・当社: アプリケーション層のセキュリティ対策、AWS 設定の適切な管理

・AWS: インフラの物理的・論理的セキュリティ

2. 可用性(共同責任)

・利用者:推奨環境での利用、計画停止時間の考慮

・当社: 仮想環境システム、アプリケーションの冗長構成、障害検知、復旧手順

・AWS: インフラの 99.99%稼働率保証(SLA に基づく)

■責任分界点表

セキュリティ領域	利用者責任	当社責任	AWS 責任
物理セキュリティ	−	−	データセンター全般
ネットワーク	接続元 IP 管理	VPC 設計、SG/NACL 設定	物理ネットワーク
サーバー	−	ゲスト OS、ミドルウェア	ハイパーバイザー
アプリケーション	適切な利用	開発、運用、脆弱性対応	−
データ	データ品質、適法性	暗号化実装、バックアップ	ストレージ基盤
認証・認可	認証情報管理	IAM ポリシー設計	IAM 基盤
暗号化	−	暗号化設定、鍵管理	KMS 基盤
監視・ログ	−	ログ設定、分析、保管	CloudWatch/Trail 基盤

■ インシデント発生時

1. AWS インフラ起因の障害
   ・AWS 障害検知、初期対応、AWS Health Dashboard での通知
   ・当社: AWS からの情報収集、影響範囲確認、利用者への通知
   ・利用者: 通知受領、必要に応じた対応
2. 本サービス起因の障害
   ・当社:障害検知、原因調査、復旧作業、利用者への通知
   ・利用者: 通知受領、影響確認
3. 利用者起因の問題
   ・利用者: 問題の報告
   ・当社: 問題の切り分け、助言
   ・利用者: 必要な対応実施

■ AWS 認証・コンプライアンスの活用

1. AWS が取得している認証
   ・ISO 27001/27017: AWS データセンターで取得済み
   ・SOC 1/2/3: AWS 側で定期監査実施
   ・PCI DSS: AWS 基盤で認定取得
   ・ISMAP:日本政府クラウドサービス認定(AWS 東京リージョン
   ※当社は、これら AWS 認証を基盤として、上位層(アプリケーション層)での ISO 27001/27017 認証を取得することで、エンドツーエンドのセキュリティを保証。

■ 定期的な責任分担の確認

頻度: 年 1 回または重要な変更時

レビュー項目

・AWS サービスアップデートによる責任変更
・新規 AWS サービス採用時の責任明確化
・法規制変更への対応
・インシデントから得られ対策の反映
・当社、外部 IT サービスチェックリストにて現状再確認

■責任の遂行に関する留意事項

1. 不可抗力免責
   当社の合理的管理を超える状況(不可抗力、政府機関の行為、洪水、火災、地震、暴動、テロ行為ストライキ、インターネットサービスプロバイダの障害、非アプリケーション又はサービス拒否(DoS)攻撃など)により生じた稼動停止については、当社は責任を負いません
2. 第三者責任
   利用者等が本サービスと共に利用する第三者サービスに起因する問題については

利用者等が当該第三者サービスの提供者との間で解決するものとします

3. 連携責任

当社・利用者等・AWS の三者が適切に連携し、それぞれの責任範囲を遂行することで
安全かつ安定的なサービス提供を実現します。

7.2.2 情報セキュリティの意識向上，教育及び訓練

SPCC では、ISO/IEC27001 を取得しており、従業員に対し情報セキュリティ教育を実施しています。

利用者が本サービスを利用するにあたり、その従業員に対する教育を補助するために、サービスの操作マニュアルなどを提供します。

8.1.1 資産目録

本サービスは、利用者から個人情報を預かりません。
利用者から受領した会話録音データは、当社にて個人情報を本サービスにて削除し
加工データとして利用します。当社にて個人情報は保持いたしません。
本サービスの特性上、本サービス上で利用するデータには個人情報は含まれません。

ただし、利用者のデータ不備により、誤って個人情報が含まれる可能性があります。
その場合、個人情報の管理責任は利用者に帰属し、
当社は技術的・物理的な安全管理措置を提供する立場となります。
誤って個人情報が含まれる場合の責任分界
- 利用者の責任：個人情報保護法の遵守、適切な入力・管理、利用目的の特定など
- 当社の責任セキュリティ対策：アクセス制御、暗号化、バックアップなど

CLD.8.1.5 クラウドサービスカスタマの資産の除去

利用者が本サービス上で入力されたデータの所有権は、全て利用者に帰属します。したがって利用者の許可なく当社がその情報を使用することはございません。

契約終了後、翌日から本サービスへのアクセスは停止されます。
利用者にて入力されたデータ・バックアップは、30 日後完全に消去します。
ご契約期間中のバックアップデータの保存期間は 3 カ月間になります。
バックアップデータも契約終了後、30 日後完全に消去します。

データ削除後の保持期間

詳細は、本サービス仕様書の「データ消去」と「ログ取得と保管」ご参照ください。

8.2.2 情報のラベル付け

保存されたデータに対してラベル付けを行う機能は提供しておりません。

9.2.1 利用者登録及び登録削除

本サービスは、お客様環境から当社提供のプログラムにより、
データを自動的にアップロードする方式を採用しているため、利用者アカウントの概念は存在せず、
本項目は該当いたしません。

9.2.2 利用者アクセスの提供

本サービスは、プログラムベースのデータ送受信方式であり、
個別の利用者に対するアクセス権限の付与は行っておりません。
本項目は該当いたしません。

9.2.3 特権的アクセス権の管理

本サービスは、プログラムによる自動アップロード・ダウンロード方式のため、
お客様側において特権的アクセス権限を管理する対象は存在しません。
本項目は該当いたしません。

9.2.4 利用者の秘密認証情報の管理

ログイン認証方式はプログラムに組み込まれたアクセスキーによる認証と
グローバル IP アドレスによる制限により管理されます。

9.2.5 当社、本サービス担当者のアクセス認証情報の管理

ログイン認証方式は ID・パスワード方式やその他セキュアな接続方法を組み合わせて運用しています。
当社、情報セキュリティポリシーで定めた管理体制に沿って、データにアクセスできる管理者を
制限しております。

9.4.1 情報へのアクセス制限

クラウドサービス上のクラウドサービスカスタマデータへのアクセス

当社によるアクセス

原則としてお客様データにアクセスしません。
障害対応・調査時のみ、お客様の事前了承を得てアクセスします。
すべてのアクセスはログ記録・監査を実施。

お客様のアクセス

本サービスを介してのみデータアクセス可能
管理者権限アカウント：管理者権限アカウントの提供はありません。
ユーザ権限アカウント：解析用源泉データのアップロード、およびレポート DL のみ可能
※本サービスへのアクセスは、利用者専用のプログラムを当社から提供いたします
そのプログラムからのみデータ送受信が可能になります。

9.4.4 特権的なユーティリティプログラムの使用

特権的なユーティリティプログラムは提供範囲外となります。

CLD.9.5.1 仮想コンピューティング環境における分離

クラウドサービスカスタマが本サービスにて利用する仮想マシンやネットワークは、AWS 上のセキュリティグループにて論理的に分離されています。

CLD.9.5.2 仮想マシンの要塞化

クラウドサービスカスタマの利用する仮想環境は、WAF やネットワーク分離、各ログ記録等、
各クラウドサービスにセキュリティ対策が施されています。

10.1.1 暗号による管理策の利用方針

クラウドサービス上のデータ通信及びデータ保管は、以下の暗号化技術で自動的に暗号化されます。

データ通信

暗号化方式	国際標準プロトコルの採用 最新の業界標準暗号化プロトコルを採用 強固な暗号化方式により、通信内容の機密性と完全性を確保 定期的なセキュリティ評価に基づくプロトコルの最適化
暗号鍵の種類	高度な暗号化技術 256 ビット暗号化を含む、業界最高水準の暗号強度を実装 複数の暗号化方式の組み合わせによる多層防御
証明書とデジタル認証	認証局により発行された正規のデジタル証明書を使用 証明書の自動更新により、常に有効な認証状態を維持 厳格なアクセス制御のもとでの証明書管理
暗号鍵の管理	クラウドサービスプロバイダの専用セキュリティサービスを活用した鍵の保護 SSL のプライベート暗号鍵は、セキュリティーチームにより、セキュアな環境で厳重な 管理をされています。暗号鍵にアクセスできる人間は限定されており、そのアクセスロ グは記録されています。また、暗号鍵に関する管理手順（生成、使用、保存、バックアップ、リカバリ、削除）などを定めています。

データの保管

暗号化方式	国際標準として広く採用されている 256 ビット暗号化方式を使用 データの機密性と完全性を同時に保証する認証付き暗号化技術を採用
暗号鍵の種類	共通鍵、対称鍵
暗号鍵の強度	現在の技術では事実上解読不可能な暗号強度を実現 国際的なセキュリティ認証基準を満たす暗号化レベル
暗号鍵の管理	AWS の専用鍵管理サービスを活用 高度なセキュリティ環境下での暗号鍵の保護 暗号鍵へのアクセスは、職務上必要な最小限の管理者のみに厳格に制限

11.2.7 装置のセキュリティを保った処分又は再利用

AWS 環境では、ストレージメディアの物理的な処分や再利用は AWS の責任範囲となります。
AWS は、業界標準に準拠した厳格なプロセスに従い、使用済みストレージメディアの安全な廃棄・再利用を実施しています。
具体的には、AWS 側で以下の対応がなされています。

使用済みストレージデバイスは、AWS 独自の廃棄プロセスに従って処理され、NIST 800-88 のメディアサニタイゼーションガイドラインに準拠した方法で完全に消去されます。

物理的に破壊する必要がある場合は、安全な方法で実施され、すべての廃棄プロセスは記録・検証されます。

AWS はこれらのプロセスを第三者監査機関によって定期的に監査され、ISO 27001、ISO 27017、PCI DSS 等の国際標準に準拠していることが確認されています。

当社の責任範囲としては、AWS 上に保存するデータの分類とライフサイクル管理ポリシーを適切に設計・実装し、不要になったデータを適切に削除することで、クラウド上のデータセキュリティを確保しています。

12.1.2 変更管理

クラウドサービスカスタマに何らかの影響が発生する可能性のある変更及びメンテナンスについては
事前にメールにて変更実施の 7 営業日前までに通知を行います。
随時メンテナンス等は、本サービス仕様書をご参照ください。

12.1.3 容量・能力の管理

本サービスでは、利用者が容量や能力を意識することなくサービスをご利用いただけるよう、インフラストラクチャの容量・能力管理を完全に当社が担っています。

具体的な取り組みとしては
プラットフォーム全体の使用状況を常時監視し、処理能力、ストレージ容量、ネットワーク帯域など、すべての重要リソースを自動的に追跡しています。

高度な予測分析と使用パターンの評価に基づき、需要の増加に先立ってインフラストラクチャを計画的に増強しています。

冗長性と高可用性を考慮した設計により、単一障害点を排除し、サービスレベル目標（SLO）を一貫して達成できる環境を維持しています。

ISO 27017 に準拠した厳格なセキュリティ管理のもと、リソースの追加・変更プロセスを実施しています。

定期的な容量レビューと継続的改善プロセスにより、パフォーマンスとコストの最適バランスを追求しています。

利用者はこれらの詳細を意識することなく、本サービスをご利用いただけます。

CLD.12.1.5 実務管理者の運用のセキュリティ

お客様環境の保護（誤操作リスクの排除）

本サービスでは、お客様の誤操作による重大な影響を防ぐため、サービスに重大な影響を及ぼす
可能性のある管理者権限機能は、お客様には提供しておりません。
システムの安定性と安全性を確保するため、これらの操作は当社の厳格な管理体制のもとで
当社担当者にて実施されます。

12.3.1 情報のバックアップ

本サービスの利用者データは毎日無停止でバックアップを実施しています。
本サービスのバックアップデータから利用者のデータ削除等による任意の復旧は致しません。
詳細は、本サービス仕様書のバックアップをご参照ください。

12.4.1 イベントログ取得

- 本サービスの取得対象ログ種別

  アクセスログ：本サービスへのアクセス履歴

- 取得方法

  本サービスでは、セキュリティおよび運用上の目的で上記ログを取得・保管しています。

- お客様へのログ提供について

  本サービスのログおよび本サービスの AWS 基盤上のログは、当社セキュリティポリシーに基づき
  原則として利用者等への直接提供は行っておりません。
  ただし、監査、コンプライアンス、インシデント調査等の正当な目的がある場合は、
  情報セキュリティを損なわない範囲で、協議の上で必要最小限の情報開示を検討いたします。

※本サービスにおけるログの取得、保存期間、保存方法および目的の詳細については、
当社が別途定める「感情カルテサービス仕様書」をご参照ください。

12.4.4 クロックの同期

本サービス及び AWS 環境のクロック同期、AWS が提供している
Amazon Time Sync Service にて高精度かつ信頼性の高い NTP サービスと同期しています。
日本標準時（JST）の正確な時刻同期が確保されています。

CLD.12.4.5 クラウドサービスの監視

AWS 環境におけるクラウドサービスの監視については、責任共有モデルに基づき、以下のように実施しています。

AWS 環境では、AWS 提供の包括的なモニタリングサービスと、当社独自の監視ツールを組み
合わせた多層的な監視体制を構築しています。

・インフラストラクチャレベルの監視
・ネットワーク監視
・システム稼働監視

・セキュリティ監視
・アプリケーション監視
・ユーザー体験の品質監視
・統合監視ダッシュボード
・インシデント対応

監視で検出した異常は、重大度に応じたエスカレーションプロセスに従って対応し
自動通知システムを構築。また、収集したモニタリングデータは定期的に分析し
リソース最適化やセキュリティ強化に活用。
なお、AWS 環境インフラ自体の監視・運用は AWS の責任範囲となりますが、当社が構築した
AWS 上のシステムについては、上記の監視体制により高可用性と安全性を確保しています。

12.6.1 技術的ぜい弱性の管理

AWS 環境における技術的脆弱性の管理については、責任共有モデルに基づき、以下のように実施しています。

責任範囲の明確化

AWS 基盤インフラ（物理的セキュリティ、ネットワークインフラ、仮想化層）の脆弱性管理は
AWS の管理になります。
当社は AWS 上に構築したシステム（OS、ミドルウェア、アプリケーション、設定）の脆弱性管理を
担当になります。

脆弱性の検出と評価

サードパーティ製脆弱性スキャンツールを活用し、定期的な脆弱性診断を定期実施
脆弱性診断として、プラットフォーム診断と Web アプリケーション診断を定期実施

脆弱性情報の収集

AWS 関連の脆弱性情報の定期的確認
JPCERT/CC、ベンダー情報など外部情報源からの脆弱性情報の定期収集
重大な影響を与える脆弱性が検知された場合には、当社から利用者へメールにて通知します。

パッチ管理と修正プロセス

計画的パッチ適用の実施し、また重大な脆弱性に対しては緊急パッチ適用プロセスを整備

変更管理との統合

セキュリティパッチ適用は変更管理プロセスと統合
テスト環境での検証後、本番環境へのパッチ適用を実施

インシデント対応と報告

本サービスに重大なセキュリティ脆弱性が検出された場合は、当社から利用者へメールにて通知し
脆弱性に対する緩和策及び根本対策を実施しています。

13.1.3 ネットワークの分離

AWS 環境におけるネットワークの分離については、AWS が提供する強固な論理分離技術を基盤とし、以下の多層防御アプローチによってマルチテナント環境における安全なネットワーク分離を実現しています。

・仮想ネットワーク

各利用者用の論理的に完全分離されたプライベートネットワーク環境を構築しています。

・アクセス制御

最小権限の原則に基づき、必要最小限の通信経路のみを許可

・アプリケーション層の保護御

アプリケーション層におけるマルチテナントの分離

一般的なウェブ攻撃からのアプリケーション保護

CLD13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合

AWS 環境におけるネットワークセキュリティ管理については、AWS の責任共有モデルに基づき以下のように実装しています。

ネットワーク分離とアクセス制御

本サービス提供環境と管理環境を完全に分離し、目的に応じた適切なセキュリティレベルを維持しています。

脅威防御

マルウェア対策、Web アプリケーション保護、メール認証など、複数のセキュリティ層を組み合わせた防御体制により、多様なサイバー脅威からシステムを保護しています。

統合監視体制

ネットワークトラフィックの継続的な監視により、セキュリティインシデントを早期に検知します。

定期的な脆弱性評価とセキュリティパッチの適用により、常に最新のセキュリティレベルを維持しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

本サービスの情報セキュリティ要求事項の分析及び仕様化について以下のように対応しています。

包括的なセキュリティ情報提供

当社の「セキュリティポリシー」において、AWS 基盤上で構築したサービスのセキュリティ管理体制、責任範囲、および対策を実施しています。

責任共有モデルの明確化

AWS 責任範囲：インフラストラクチャ、ネットワーク、ハイパーバイザー層のセキュリティ

当社責任範囲：アプリケーション、データ、アクセス管理、設定管理

セキュリティ要求事項の継続的な分析と更新

脅威情報の継続的な収集と分析

透明性の確保*

重要なセキュリティアップデートや変更に関する利用者への事前通知体制

インシデント発生時の適切な情報開示ポリシーの整備

本サービスの各種セキュリティ仕様は、本サービス仕様書「セキュリティ」をご参照ください。

14.2.1 セキュリティに配慮した開発のための方針

AWS 環境におけるセキュリティに配慮した開発のための方針について、以下のように実装しています。

ガイドラインの整備と運用

当社の「情報セキュリティ基本規程」および「情報システム管理マニュアル」を基本とし
当社の開発ガイドラインに則って開発を行っています。

安全な開発環境の維持

開発環境と本番環境の完全分離

AWS IAM を活用した最小権限の原則に基づく開発者アクセス制御

15.1.2 供給者との合意におけるセキュリティの取扱い

クラウドサービスプロバイダとして、クラウドサービスの提供及び利用者に対しては当社の「セキュリティポリシー」に記載しております。

なお、責任分界点についての解説は、前出の「責任分界点について」の項を参照ください。

15.1.3 ICT サプライチェーン

当社からの委託先については、契約約款の定めにしたがい管理を行っています。

本サービスの開発・運用・保守・販売活動を当社内で完結しており

AWS 基盤を活用した ICT サプライチェーン管理として以下を実施しています:

AWS 供給者管理

AWS サービスレベル合意（SLA）の定期的評価

AWS コンプライアンスプログラム（SOC、ISO 認証等）の確認

16.1.1 責任及び手順

当社で確認できたセキュリティインシデントについては、別紙:「感情カルテ_情報セキュリティ基本方針」に従い、対応・周知いたします。確認できたセキュリティインシデントが、利用者に影響を及ぼす可能性がある場合は、

当社担当から利用者へメールにて通知いたします。

16.1.2 情報セキュリティ事象の報告

利用者が発見した情報セキュリティ事象の報告や、その他の問い合わせ、報告は、当社担当へ

ご連絡いただくか、感情カルテお問い合わせ窓口 karte_support_abc@spcc-sp.com へメールにて

ご連絡ください。

報告後の対応

受付確認後、当社担当にて調査を実施し、影響範囲の特定と分析

責任分界点に応じた対応（AWS 起因の場合は AWS サポートと連携）

解決策と対応結果をメールにて回答

16.1.7 証拠の収集

本サービスと AWS 環境における法的対応と証拠収集については

本サービス利用規約の「デジタルフォレンジックを支援するための情報共有と法的対応」をご参照ください。

18.1.1 適用法令及び契約上の要求事項の特定

当社および本サービスと AWS 環境における法的フレームワーク

準拠法

本サービスは日本法に準拠します。

AWS 日本リージョンを基盤として利用し、データ所在地を日本国内に維持

AWS 特有の規制対応

AWS 日本リージョンは日本の各種法令（個人情報保護法、電気通信事業法等）に対応。

AWS 責任共有モデルに基づき、インフラ層のコンプライアンスは AWS が、アプリケーション層・データ層のコンプライアンスは当社が責任を負います。

18.1.2 知的財産権

本サービスの知的財産権と保護は、当社が全ての知的財産権を保有します。

利用者から問い合わせは、当社担当へご連絡いただくか

感情カルテお問い合わせ窓口 karte_support_abc@spcc-sp.com へメールにてご連絡ください。

18.1.3 記録の保護

当社の責任範囲において、各種アクセスログ、システムログを取得・保管しています。

ログ関連の詳細は、本サービス仕様書のログ管理をご参照ください。

18.1.5 暗号化機能に対する規制

国内の暗号化機能に対する規制に準拠する必要があります。

日本国内の暗号化規制対応

本サービスは、AWS サービスは国内の暗号化機能規制に準拠

18.2.1 情報セキュリティの独立したレビュー

ISO/IEC 27001 および ISO/IEC 27017 について第三者による審査を受け、認証取得することで、情報セキュリティに対する取り組みの証憑とし、クラウドカスタマの求めに応じて開示します。

社内の内部監査委員会に社外の第三者を加えた監査チームによる内部監査を年 1 回実施し監査結果についてレビューを行い証憑として保管します。

以上