情報区分	公開
発　効　日	2023/03/09
版　番　号	Ver.4.1

スマートコンタクトセンター（SCC）
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

改訂履歴表

版番号	発効年月日	改　訂　内　容
Ver.1.0	2018/9/1	新規制定
Ver.2.0	2019/11/15	情報区分を公開に変更、責任分界点修正
Ver.3.0	2022/3/28	バックアップ保存先から米国の記載を削除
Ver.4.0	2022/12/15	「ホワイトペーパーの目的/4ページ」URL変更 (変更前)https://www.spcc-sp.com/SCC/ (変更後)https://www.spcc-sp.com/compliance/
Ver.4.1	2023/03/09	14.2.1 セキュリティに配慮した開発のための方針 開発ガイドラインを追記

目次

はじめに

ホワイトペーパーの目的

このホワイトペーパー（以下、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/IEC27017:2015）」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、スマートコンタクトセンター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/IEC27017:2015 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、スマートコンタクトセンター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、スマートコンタクトセンターの取り組みは、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、スマートコンタクトセンターサービスとなります。

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 27017:2015 および JIS Q 27017:2016 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 27017:2015 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/IEC27001:2013 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/IEC27002:2013 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/IEC27017:2015 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/IEC27017:2015 は、

ISO/IEC27002:2013 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/IEC27017:2015 は、JIS Q 27017:2016 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 27017:2015）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 27017:2015 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。

スマートコンタクトセンターサービスについて

スマートコンタクトセンターサービスについて

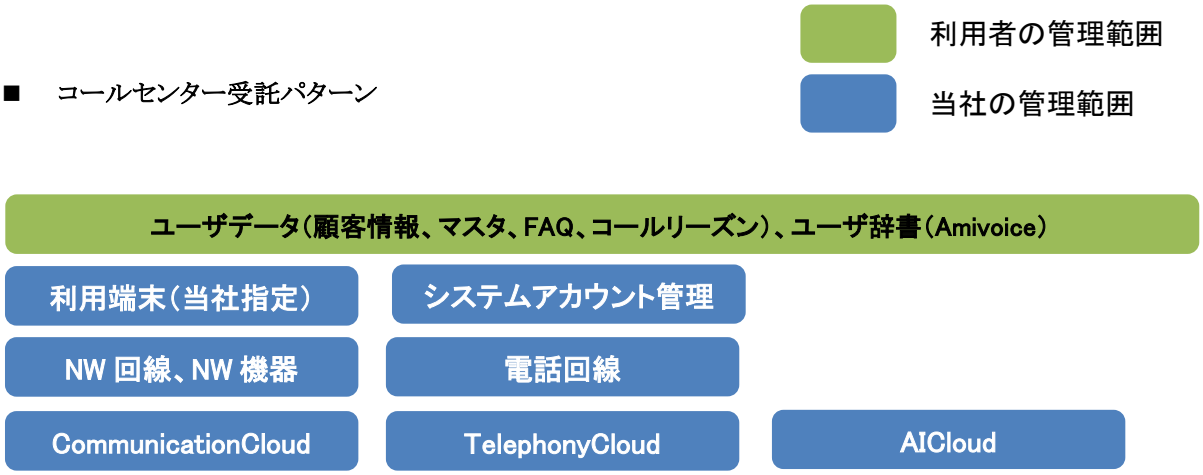
スマートコンタクトセンターはパブリッククラウドに分類される CCaaS（Contact Center as a Service)のサービスです。

スマートコンタクトセンターにはさまざまな機能が備わっていますが、コンタクトセンターとして利用するうえで最も基本的な機能を『スマートコンタクトセンターサービス』として提供しています。

責任分界点について

スマートコンタクトセンターサービスに関する責任分界点は、以下のようになります。

■　コールセンター受託パターン



■　システム提供パターン　※現状はサービス提供の予定なし

JIP-ISMS517-1.0、ISO/IEC 27017:2015 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『スマートコンタクトセンターサービス』と定めています。

ISO/IEC 27017:2015（JIS Q 27017:2016）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「情報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、「情報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お客様に提供すること。
2. お客様に、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 SCC 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。

■お客様の責任

お客様は、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、及びお客様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. お客様が本サービス又は本コンテンツと共に利用する非 SCC 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

お客様のデータはすべて、日本にある各クラウドサービス毎のデータセンターに保管されています。

オムニチャネル基盤	Salesforce（日本にあるメインセンター）
テレフォニー基盤	BellCloud データセンター（豊洲 DC、北九州 DC)
AI 基盤	AWS（東京リージョン）

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

1. お客様は、当社提供物を善良なる管理者の注意をもって管理するものとします。
2. お客様は、本サービスを利用した一切のお客様等の行為及びその結果について一切の責任を負い、当社に対していかなる迷惑及び損害も与えないものとします。
3. お客様は、本サービスを通じてお客様等が発信した情報について一切の責任負うものとし、当社に対していかなる迷惑及び損害も与えないものとします。
4. 前 2 項に定める事由より、当社が損害を蒙った場合には、お客様その損害を賠償するものとします。
5. お客様は、本サービスの利用に関して本件第三者等に対して損害を与えた場合、自己の責任と負担において当該損害を賠償するものとします。

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。

お客様がスマートコンタクトセンター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

SCC では、カスタマから預かった顧客情報とアカウント情報を資産対象と定義する。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

お客様がスマートコンタクトセンターサービス上で入力されたデータの所有権は、全てお客様に帰属します。したがってお客様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 30 日以内にお客様からの申し出があれば、全てのデータは返却されます。

お客様からの直接の申し出がない場合、解約後も 180 日間はディスク上にデータを保持しています、180 日後にデータは論理削除され、さらに 30 日後に他のデータで上書きされます。

バックアップについては、最も古いもので 90 日前のものであり、90 日間でバックアップテープを含めすべての媒体からデータが削除されます。

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

1. アカウントの登録に必要な情報は、氏名、部署名、メールアドレス、従業員番号等です。
2. アカウントの登録申請は、当社で提供する申請書にて登録・削除が可能です。

9.2.2 利用者アクセスの提供(provisioning)

提供するユーザーのアクセス権は以下となります。

- 管理者ユーザー（SV）
- 一般ユーザー（CSR）

9.2.3 特権的アクセス権の管理

システムに対する特権ユーザーは提供範囲外となります。

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 ID・パスワード方式のみとなります。

ただし、プロファイルごとにアクセス元 IP アドレスによるログイン制限を施すことが可能です。

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を制限することが可能です。

提供するユーザーのアクセス権は以下となります。

- 管理者ユーザー（SV）
- 一般ユーザー（CSR）

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の利用する仮想マシンやネットワークは、VLAN によっ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

ファイアーウォールやログ記録等、各クラウドサービス毎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	AES_256_CBC
暗号鍵の種類	共通鍵
暗号鍵の強度	2048bit
暗号鍵の管理	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	128bit AES(Advanced Encryption Standard)
暗号鍵の種類	共通鍵
暗号鍵の強度	
暗号鍵の管理	非常に限定されたデータベース管理者以外にはアクセスはできません。

11.2.7 装置のセキュリティを保った処分又は再利用

使用している記憶媒体については、RAID により冗長化された領域に、仮想のストレージ領域を保持しているため、ストレージを構成する HDD を一つだけ取得しても、中の情報が取り出せない状態になっています。なお、故障等により交換した記憶媒体の処理については、当社と機器ベンダーとの契約に基づき適切に処理を行っています。

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、事前にメール及びポータルサイトにて、原則として 14 日前までに通知を行います。

12.1.3 容量・能力の管理

サービススペックを明確にするとともに、各種リソースについて常に監視を行っております。

また、各種リソースについてのお問い合わせにつきましては、現在の利用状況や拡張の手続き方法を提供することが可能です。

CLD.12.1.5 実務管理者の運用のセキュリティ

クラウドサービスの誤操作により大きな影響を及ぼすデバイスの変更や削除等の管理者権限の操作機能は提供致しません。

12.3.1 情報のバックアップ

クラウドサービス上のデータのバックアップ範囲は以下になります。それぞれのバックアップ方法、復元方法については、スマートコンタクセンターバックアップ仕様書を参照してください。

① CRM サービス上のお客様データ、CRM サービスに付随する設定情報、CRM サービスに関するシステムデータ
② PBX 関連の設定データ
③ 通話録音データ
④ AI 応答補助サービスに付随するシステムデータ

12.4.1 イベントログ取得

- 取得対象ログ種別
  1. CRM サービスへのログイン履歴、設定変更履歴
  2. CRM サービスの各レコードの作成日、更新日、最終更新者
  3. CRM サービスアプリケーションに対するアクセスログおよび、データベース、ルーター、ファイアーウォール、IDS などのシステムログ
  4. 音声基盤システム上のアラーム、エラー、イベント、設定変更などのシステムログ
  5. AI 応答補助サービスにおける管理コンソール操作ログ
- 取得方法
  1. 「CRM サービスへのログイン履歴、設定変更履歴」はお客様からのお申し出から翌営業日までに提供
  2. 「CRM サービスの各レコードの作成日、更新日、最終更新者」はお客様からのお申し出から翌営業日までに提供
  3. 「CRM サービスアプリケーションの各種システムログ」は有償にて提供可能です。
  4. 「音声基盤システム上の各種ログ」 は問題発生時等の調査で利用致しますが、お客様への開示はしておりません
  5. 「AI 管理コンソールログ」 はお客様からのお申し出から翌営業日中に提供

12.4.4 クロックの同期

お客様ご自身で日本標準時に合わせて使用してください

CLD.12.4.5 クラウドサービスの監視

運用監視ツールを用いてシステム監視を行っています。

- 監視対象および内容
  a. ネットワーク機器
  b. サーバー機器
  c. ストレージ機器
  d. 基本ソフト(オペレーティングシステムやデータベースソフト)
  e. システムサービス(システムの機能を補佐するプロセス／プログラム)
  f. アプリケーションプロセス(業務処理を行うプロセス)　等

上記の監視対象に対して、それぞれの稼働状況、資源の使用状況、パフォーマンス状況、特定のイベント・メッセージ（例：アクセス違反など）とその急激な増加・減少などを監視しています。

12.6.1 技術的ぜい弱性の管理

リリース前および、定期的な脆弱性診断の実施や、定期的なネットワーク診断を行っています。

また、ぜい弱性情報の収集を行い、対策を行っています。

SCC のサービスにおいて重大な影響を与える脆弱性が検知された場合には当社の管理するポータルサイトにて報告します。

13.1.3 ネットワークの分離

論理的な隔離によるマルチテナント化を実現しています。

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

SCC クラウドサービスでは目的ごとにネットワーク領域を分離し、運用しています。ネットワークの設定は物理と仮想において整合性を保っています。SCC のサービス管理のためのネットワークはユーザーのサービス利用のものとは分離しています。また、必要な通信のみを許可し、ウイルス対策ソフトや不正アクセス検知装置、迷惑メールフィルタ等の技術的な対策を実装しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

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。

また、当クラウドサービスの各種セキュリティ機能は、SCC サービス仕様書にて、問い合わせに応じて提示致します。

14.2.1 セキュリティに配慮した開発のための方針

定期的な脆弱性診断の実施や、定期的なネットワーク診断を実施しております。

このサービスは、当社の開発ガイドラインに則って開発を行っています。

ガイドライン「情報セキュリティ基本規程」「情報システム管理マニュアル」。

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。

16.1.1 責任及び手順

弊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:「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、お客様に影響を及ぼす可能性がある場合は、SCC ポータルサイトにて周知いたします。

16.1.2 情報セキュリティ事象の報告

お客様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、ポータルサイトにログインした上で、チケットを起票することで行なえます。

チケット形式となっていますので、ポータルサイト上で問い合わせの履歴を追跡できます。

16.1.7 証拠の収集

捜査機関または監督官庁より指導、摘発、注意もしくは照会を受けた場合は、クラウドサービスカスタマへの通知および同意を経ることなく、当該機関に情報を開示することについて、契約書にて合意いただく必要があります。

18.1.1 適用法令及び契約上の要求事項の特定

準拠法は日本法です。

18.1.2 知的財産権

クラウドサービスカスタマからの問い合わせは、ポータルサイト上からチケットの起票によって行うことができます。

18.1.3 記録の保護

弊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。

保存方法、保存期間、取得の方法など、詳細については、スマートコンタクセンターログ仕様書を参照してください

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。

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。