KISSEI COMTEC

S3-5007-02

ペーパーレス会議システム

Smart Discussion

スマートディスカッション

クラウドセキュリティホワイトペーパー

第 2 版

2026 年 10 月 発行

目次

1. このホワイトペーパーについて 1
2. 本書の適用範囲について 2
3. ISO / IEC 27017 について 3
4. クラウドサービスの管理策 4
A.5.1.1 クラウドセキュリティの方針群 4
A.6.1.1 クラウドセキュリティの役割および責任 4
A.6.1.3 関係当局との連絡 5
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共有及び分担 5
A.7.2.2 情報セキュリティ意識向上、教育および訓練 5
A.8.1.1 資産目録 5
CLD.8.1.5 クラウドサービスカスタマの資産の除去 5
A.8.2.2 情報のラベル付け 6
A.9.2.1 お客様登録及び登録 6
A.9.2.2 お客様アクセスの提供 6
A.9.2.3 特権的アクセス権の管理 7
A.9.2.4 利用者の秘密認証情報の管理 7
A.9.4.1 情報へのアクセス制限 7
A.9.4.4 特権的ユーティリティプログラムの使用 7
CLD.9.5.1 仮想コンピューティング環境における分離 8
CLD.9.5.2 仮想マシンの要塞化 8
A.10.1.1 暗号化による管理策の利用方針 8
A.11.2.7 装置のセキュリティを保った処分又は再利用 9
A.12.1.2 変更管理 9
A.12.1.3 容量・能力の管理 9
CLD.12.1.5 実務管理者の運用のセキュリティ 9
A.12.3.1 情報のバックアップ 9
A.12.4.1 イベントログ取得 10
A.12.4.3 実務管理者及び運用担当者の作業ログ 10
A.12.4.4 クロックの同期 10
CLD.12.4.5 クラウドサービスの監視 10

A.12.6.1　技術的脆弱性の管理 10
A.13.1.3　ネットワークの分離 11
CLD.13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合..... 11
A.14.1.1　情報セキュリティ要求事項の分析及び仕様化..... 11
A.14.2.1　セキュリティに配慮した開発のための方針..... 11
A.15.1.2　供給者との合意におけるセキュリティの取扱..... 11
A.15.1.3　ICT サプライチェーン 12
A.16.1.1　責任及び手順 12
A.16.1.2　情報セキュリティ事象の報告..... 12
A.16.1.7　証拠の収集..... 12
A.18.1.1　適用法令及び契約上の要求事項の特定 12
A.18.1.2　知的財産権..... 12
A.18.1.3　記録の保護..... 13
A.18.1.5　暗号化機能に対する規則..... 13
A.18.2.1　情報セキュリティの独立したレビュー 13
5.　改訂履歴 14

1. このホワイトペーパーについて

このホワイトペーパー（以下、本書）は、キッセイコムテック株式会社（以下、当社）が提供するペーパーレス会議システム Smart Discussion におけるセキュリティの取り組みについて理解を深めていただくためのものです。クラウドセキュリティの国際規格 ISO/IEC 27017 の中で、お客様に向けて情報開示が求められる事項について、セキュリティの取り組みをご確認いただくことができます。

2. 本書の適用範囲について

本書は、当社のデータセンターにてクラウドサービスとして提供するペーパーレス会議システム Smart Discussion（以下、本サービス）が適用範囲となります。

3. ISO / IEC 27017 について

ISO/IEC 27017 は、国際標準化機構と国際電気標準会議の下に設置された ISO/IEC JTC 1/SC 27 小委員会により公開された国際規格です。クラウドサービスの提供および利用に適用できる情報セキュリティ管理策の指針を示しています。

本規格は、情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取り組みをクラウドサービスの観点から強化するものです。クラウドサービス提供者と利用者の双方を対象とし、それぞれの役割と責任を明確に定義しています。資産管理・アクセス制御・暗号化・インシデント対応・情報開示など幅広いセキュリティ領域をカバーしており、クラウド環境に対応した情報セキュリティ管理体制の構築と実践を支援します。

4. クラウドサービスの管理策

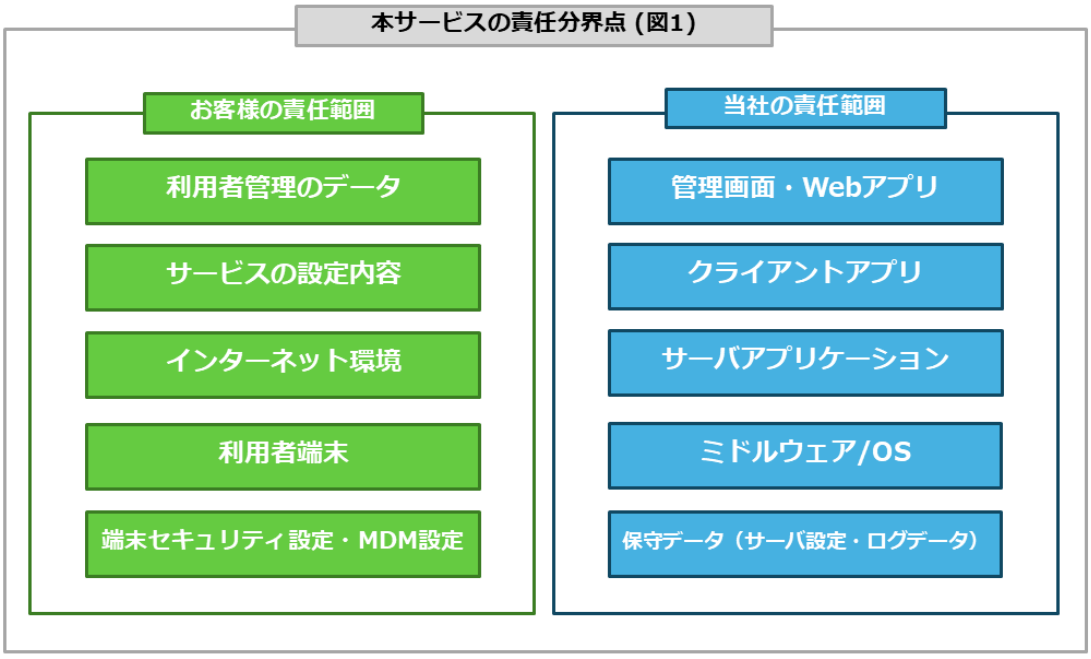
本項では、ISO/IEC 27017 管理策の実践の規範の項番に沿って本サービスの管理策を記載します。本サービスにおける ISO/IEC 27017 の定める管理項目への管理策は以下のとおりです。

A.5.1.1　クラウドセキュリティの方針群

当社は「情報セキュリティ基本方針」を定め、お客様が安心してご利用いただけるよう取り組んでおります。また、基本方針および関連する社内規則は、ISMS 活動の中で年に 1 回見直しをしております。

A.6.1.1 クラウドセキュリティの役割および責任

本サービスは、お客様と当社の情報セキュリティの責任範囲について、図 1 のとおり責任分界点を定義しております。



A.6.1.3　関係当局との連絡

当社の所在地は、当社ウェブサイトでご確認ください。
「https://www.kicnet.co.jp/abouts/」
本サービスにて保存されるデータの所在は、日本国内のデータセンターです。

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共有及び分担

本サービスは、サービスの提供環境における役割および責任について約款に定めサービスを提供します。

本サービスの責任分界点については、「6.1.1 情報セキュリティの役割および責任」をご確認ください。

A.7.2.2　情報セキュリティ意識向上、教育および訓練

本サービスでは、サービス運営担当者に対し、当社が定めたセキュリティ教育に加え、クラウドサービス運用手順書 Smart Discussion(ペーパーレス会議システム)に定めた管理事項の運営に必要な教育を実施しています。

A.8.1.1　資産目録

本サービスでは、お客様の情報資産（お客様が設定、または保存されるデータ）と当社がサービスを運用するための情報を、明確に分離しています。

お客様の情報資産に関しては、お客様の管理範囲です。

CLD.8.1.5　クラウドサービスカスタマの資産の除去

お客様が本サービスを解約された場合、解約後はサービス利用に関する下記データが削除されます。

・ユーザーアカウントデータ、ユーザーグループデータ
・資料グループデータ、フォルダデータ
・登録資料データ

・端末情報データ
・アプリ設定データ、システム設定データ（管理画面で設定可能な情報）
・サーバー操作ログ、ファイル閲覧ログ
・サーバーシステムイベントログ（専用サーバーの場合）

※マルチテナントサーバーの場合、お客様の情報資産を含まないサーバーシステムイベントログは削除の対象外です。

当社は解約日を起点として 30 日以内にお客様のデータを消去します。本サービスでは消去したデータはいかなる理由であっても復旧、復元することはできません。
解約時の削除処理はその実施内容を記録として保持します。
仮想サーバー削除が伴う場合は別途その削除記録を保持します。

A.8.2.2　情報のラベル付け

お客様が設定、登録する次のデータについて、管理を目的としたラベル付けが可能です。

- 資料グループ（名称変更、表示色変更）
- ユーザーグループ（名称変更、説明文の変更）
- フォルダ（名称変更、階層変更、表示色変更）
- 登録資料（名称変更）
- お知らせ（タイトル変更）

A.9.2.1　お客様登録及び登録

・本サービスのお客様が利用する管理者のアカウントは当社が発行します。
・Smart Discussion は、管理者がユーザーアカウントを登録、及び削除する機能を提供しています。具体的な操作手順は製品のシステム管理者マニュアルをご参照ください。

A.9.2.2　お客様アクセスの提供

・本サービスは、ユーザー権限（ユーザーのアクセス権）を管理する機能を提供しており、管理者が設定できます。管理機能の利用にあたっては、システム管理者マニュアルをご参照ください。

A.9.2.3　特権的アクセス権の管理

・本サービスでは、管理者アカウントに対して、ID／パスワード認証に加え、2 要素認証を設定できるオプションを提供しています。

A.9.2.4　利用者の秘密認証情報の管理

・本サービスでは、サービス利用開始時に管理者権限を有するアカウント情報を書面、または電子書類で提供します。
・管理者は、利用者アカウントのパスワードの初期設定、リセット、初回ログイン時のパスワード変更指定が設定、操作できます
・管理者はパスワード誤りによるアカウントロックの設定と、ロックアカウントの解除が可能です。
・パスワード管理機能の詳細は、システム管理者マニュアルをご参照ください。

A.9.4.1　情報へのアクセス制限

①クラウドサービスの環境や機能の管理
管理者が環境、機能の制限を実施できます。

②アカウントの管理
管理者が利用者アカウントの管理（登録・変更・削除）を実施できます。

③カスタマーデータの登録・参照
カスタマーデータ（会議資料、会議ファイル）の登録は、管理者によって登録権限が付与されたアカウントのみに制限されます。参照権限が付与されたアカウントでは、登録済データの閲覧だけが許可されます。

A.9.4.4　特権的ユーティリティプログラムの使用

本サービスでは、通常の操作手順またはセキュリティ手順を回避することができるユーティリティプログラムのお客様への提供はありません。

CLD.9.5.1　仮想コンピューティング環境における分離

本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、サーバーやネットワーク、ストレージをお客様ごとに論理的に分離しています。

選択するサービスによって次の違いがあります。

・Standard 版：

単一の仮想サーバーに複数のお客様が存在するマルチテナント環境です。テナント分離はアプリケーションおよびデータアクセス制御による論理分離で実現しています。

・Enterprise 版：

お客様専用の仮想サーバーで運用する環境です。ネットワークも分離されます。

両サービスに共通して管理ネットワークはお客様のネットワークと分離しており、運用担当者は利用者データを閲覧できません。

CLD.9.5.2　仮想マシンの要塞化

お客様が利用するサービスの提供に用いる仮想環境は、必要最小限の構成でサーバーを構築しております。また、本サービスをご利用いただくのに必要なポートやプロトコルへのアクセス制限を実施しております。加えてマルウェア対策ツールも導入しております。

A.10.1.1　暗号化による管理策の利用方針

① 通信経路の暗号化

サーバーシステムとの通信は SSL による暗号化を行っており、通信経路途中の盗聴、改竄を防止します。

② 文書ファイルの暗号化

サーバー、タブレット端末共に、保存する文書ファイルは AES256bit 暗号化方式で暗号化して保存します。

③ ユーザーパスワードの暗号化

データベースに記録する、お客様の各種情報（ID、各機能で利用するデータなど）は、適切

なアクセス権のもとで保管されます。但し、ユーザーパスワードは暗号化の上、データベースに保管します。

A.11.2.7　装置のセキュリティを保った処分又は再利用

本サービスでは、サービス提供に利用するクラウドサービスのデータの処分状況を正しく把握し、適切なプロセスでデータ管理を行っています。サービス提供に使用していた機器の廃棄にあたっては、ISO20000 に従い、データの消去、または機器の破壊を実施します。

A.12.1.2　変更管理

本サービスでは、定期的な保守などによりサービスを停止する場合、お客様に対して本サービスを停止する 30 日前までにお客様担当者にメールにて通知します。

本サービスで、機能、サービスのアップグレードを実施する場合は、実施日の 2 週間前までにお客様担当者にメールにて通知します。

A.12.1.3　容量・能力の管理

本サービスでは、サービス提供に利用するクラウドサービスの監視を行い、状況に応じてリソース増強を行うなど適切な運用管理を行っています。

CLD.12.1.5　実務管理者の運用のセキュリティ

・本サービスでは、サービスの利用に必要な操作手順を、マニュアルなどのドキュメントとしてサポートサイト及び Web アプリのメニューからダウンロード可能にしています。

A.12.3.1　情報のバックアップ

本サービスでは、システム(OS)全体のバックアップを日次で取得/保持しています。

・バックアップ対象： システム(OS)全体

・保持期間：1 日間

・バックアップデータ保管場所：日本

A.12.4.1　イベントログ取得

本サービスでは、サービスの維持管理に必要となる適切なログを取得しています。システム管理権限を有するお客様には、サーバー操作ログ、ファイル閲覧ログのダウンロード機能を提供しています。ログのダウンロードに必要な操作手順は、「システム管理者マニュアル」に記載しています。

A.12.4.3　実務管理者及び運用担当者の作業ログ

本サービスでは、サービスの提供に関わる作業および結果を記録し、レビューを実施しています。

A.12.4.4　クロックの同期

本サービスでは、サービス提供に必要なシステムのクロックを自社設置のタイムサーバと同期しています。タイムゾーンは JST(UTC+9)です。

CLD.12.4.5　クラウドサービスの監視

本サービスでは、システム管理者権限を有するお客様には、A.12.4.1 イベントログ取得に記した利用者のログを確認できます。加えて、システム管理者権限を有するお客様は管理画面にて、

・管理端末一覧、および端末のアクセス制御
・アカウントロックの発生状況
・データ容量に対する使用率

を確認できます。

本サービスでは、サーバーの死活監視、サービスプロセス監視、リソース監視を 1～5 分ごと監視しています。アラート発生時には運用部門への通知が行われ、影響がある場合には、速やかに対処します。

A.12.6.1　技術的脆弱性の管理

本サービスでは脆弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、当社の責任範囲において影響がある場合には、速やかに対応します。

A.13.1.3　ネットワークの分離

本サービスをご利用のお客様においては、論理的にネットワークを分離しています。サービス運営で必要となる管理ネットワークに関しても、お客様のネットワークと分離しています。

CLD.13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

本サービスでは、サービス提供に利用するクラウドサービスにおける仮想および物理ネットワークの整合を確認しています。

A.14.1.1　情報セキュリティ要求事項の分析及び仕様化

本サービスにおいて、暗号化、アクセス制御、ログ取得等の情報セキュリティ機能について本書にまとめて開示している。また、サービスの変更時には本書を適宜見直し、最新の状態を維持しています。

A.14.2.1　セキュリティに配慮した開発のための方針

当社の品質マネジメントシステムにおける開発手順に従い、情報セキュリティ目標を定めたシステム開発を実施しています。あわせて、定期的に Web アプリケーション診断を実施し、脆弱性のないシステムのリリースに務めています。

A.15.1.2　供給者との合意におけるセキュリティの取扱

本サービスは、サービスの提供環境における役割及び責任について約款に定め、約款に同意いただいた上でサービスを提供します。

本サービスの責任分界点については、「A.6.1.1 情報セキュリティの役割及び責任」をご確認ください。

A.15.1.3　ICT サプライチェーン

本サービスでは、ピアクラウドサービスプロバイダに対して、当社の情報セキュリティ方針、およびセキュリティ水準と同等かそれ以上であることを確認しています。

A.16.1.1　責任及び手順

本サービスでは、当社がシステム障害を検知した場合、連絡担当者に通知するまでの時間は、サポート提供時間内においては、障害を検知後 1 時間以内、サポート提供時間外においては、翌サポート提供日のサポート提供時間開始後 1 時間以内にお客様担当者にメールにて通知します。

本サービスでは、当社が確認したセキュリティインシデントがお客様に重大な影響を及ぼす場合、インシデント確認より 24 時間以内を目標にお客様担当者にメールにて通知を行います。

システム障害、セキュリティインシデントに関する問合せは、サポートサイトでお受けいたします。

A.16.1.2　情報セキュリティ事象の報告

本サービスでは、サポートサイトへのお問い合わせで、相互に情報のやりとりができる仕組みを提供しています。

A.16.1.7　証拠の収集

当社は、サービス内で収集するデジタル証拠となりうるデータ（ログなど）を第三者（裁判所、行政機関など）に提出する条件を約款に記載しています。

A.18.1.1　適用法令及び契約上の要求事項の特定

本サービスのご利用に関して、適用される準拠法は日本国の法令です。

A.18.1.2　知的財産権

本サービスをご利用いただく上での知的財産権に関わるご相談は、サポートサイトにてお問い合わせください。

A.18.1.3　記録の保護

本サービスでは、サーバーの操作ログに関するイベントログ、アクセスログ、アプリケーションログを取得します。

お客様が登録した資料、お客様が実施した設定、およびログデータは、不正アクセスや改竄を防ぐために適切に管理されたアクセス権の元で保管されます。

A.18.1.5　暗号化機能に対する規則

・本サービスでは、規制の対象となる暗号化の利用はありません。

A.18.2.1　情報セキュリティの独立したレビュー

当社は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受け、認証の取得状況を当社ウェブサイトで公開しています。（ISO/IEC 27017 は 2026 年 12 月に認証取得予定）

5. 改訂履歴

版数	改定日	改訂内容
1	2026 年 7 月 31 日	
2	2026 年 10 月 30 日	下記内容を更新 CLD.8.1.5 クラウドサービスカスタマの資産の除去 A.9.2.3　特権的アクセス権の管理 A.18.1.3　記録の保護

Smart Discussion クラウドセキュリティホワイトペーパー

2026 年 10 月　第 2 版

キッセイコムテック株式会社
〒390-1293　長野県松本市和田 4010-10

ご注意
(1) 本書の内容については、将来予告なしに変更することがあります。
(2) 本書の内容は万全を期して作成しておりますが、誤りまたはお気づきの点がございましたら、ご連絡くださいますようお願い致します。
(3) 本書記載の各社名、製品名は各社の商標、または登録商標です。
(4) 本書は著作権等の権利が保護されています。
(5) 本書記載内容について、文書による許諾を得ずに無断で転載、複写することは禁止されています。