CT-e1/SaaS
セキュリティガイドライン

ComDesign

Ver.1.0

目次

1 はじめに 4
1.1 目的....4
1.2 対象....4
1.3 情報セキュリティ方針....4
1.4 約款について....4
1.5 責任範囲....5
1.5.1 当社の責任....5
1.5.2 お客様様の責任....5

2 CT-e1/SaaSのセキュリティ....6
2.1 マルチテナントについて....6
2.1.1 「テナントID」について....6
2.2 サーバーセキュリティ....7
2.3 ネットワークセキュリティ....7
2.3.1 インターネット構成、VPN構成....7
2.3.2 データ通信、音声通信....8
2.4 クライアントセキュリティ....9
2.4.1 クライアントのパスワードについて....9
2.4.2 管理者機能....9
2.5 個人情報....10
2.5.1 通話録音ファイル....10
2.5.2 その他のクラウドに保存する情報....10
2.6 知的財産権....10

3 運用の流れ....11
3.1 問い合わせの流れ....11
3.1.1 メール....11
3.1.2 電話....11
3.2 障害時の流れ....11
3.2.1 お客様が検知した場合....11
3.2.2 弊社が検知した場合....12
3.2.3 その他....12

4 付録....13
4.1 障害時切り替え方針影響....13
4.1.1 CT-e1/SaaSシステム構成概要図....13
4.1.2 想定される障害パターン....13
4.2 サービス性能要件....15
4.3 セキュリティ要件詳細....16
4.4 適用法令一覧....25

更新日	更新者	更新内容
2023/11/6	内納　康夫	新規作成

1 はじめに

1.1 目的

本ドキュメントは、CT-e1/Saasの提供におけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

1.2 対象

CT-e1/SaaSの導入を検討中の方
CT-e1/SaaSを利用中の方

1.3 情報セキュリティ方針

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://comdesign.co.jp/cms/wp-content/uploads/2021/08/kihon.pdf

1.4 約款について

CT-e1/SaaSサービスの約款は、下記別紙にて定めております。
https://comdesign.co.jp/cms/wp-content/uploads/2021/08/CD_SRV310.pdf

1.5 責任範囲

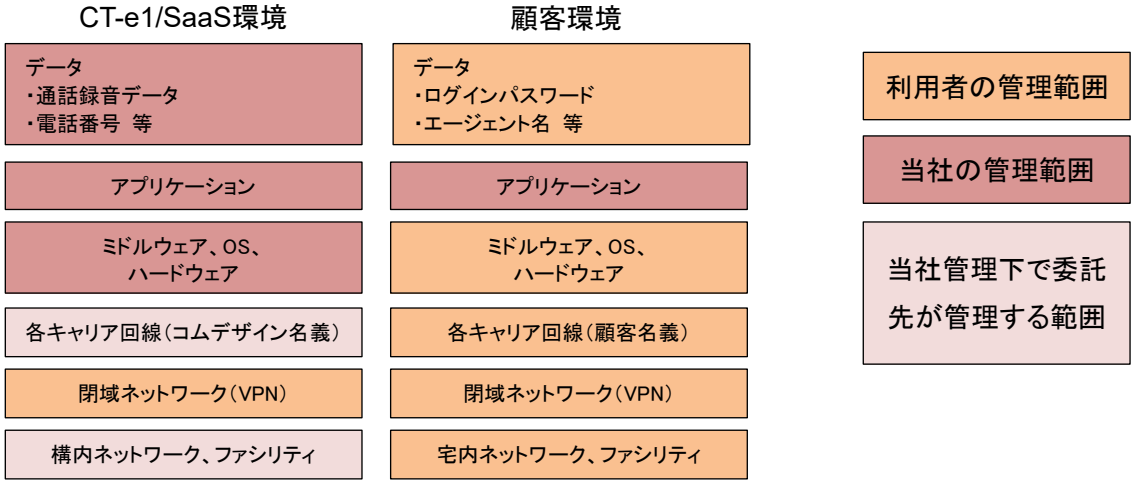
CT-e1/SaaSにおけるサービスインフラストラクチャは、当社が管理するサービス事業者によって管理されます。
また、当社は、基盤上に構築したアプリケーション及び機器に対して責任を負います。

1.5.1 当社の責任

- CT-e1/SaaSのセキュリティ対策
- CT-e1/SaaSを利用するエンドユーザーのデータの保護

1.5.2 お客様の責任

- 利用者アカウントの管理
- パスワード等の認証情報の管理
- 管理画面よりアクセス可能なデータに対してのバックアップ

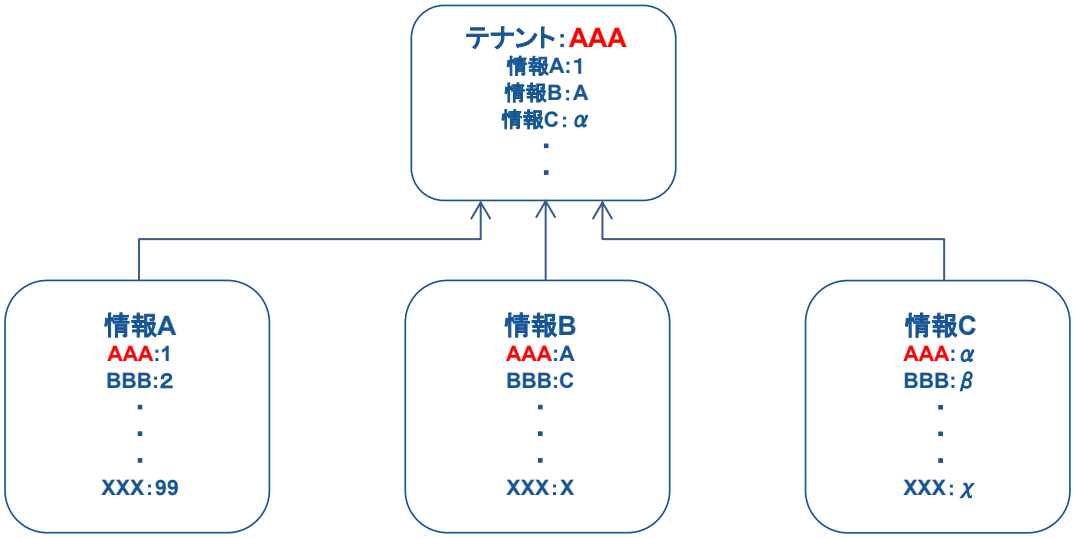


2 CT-e1/SaaSのセキュリティ

2.1 マルチテナントについて

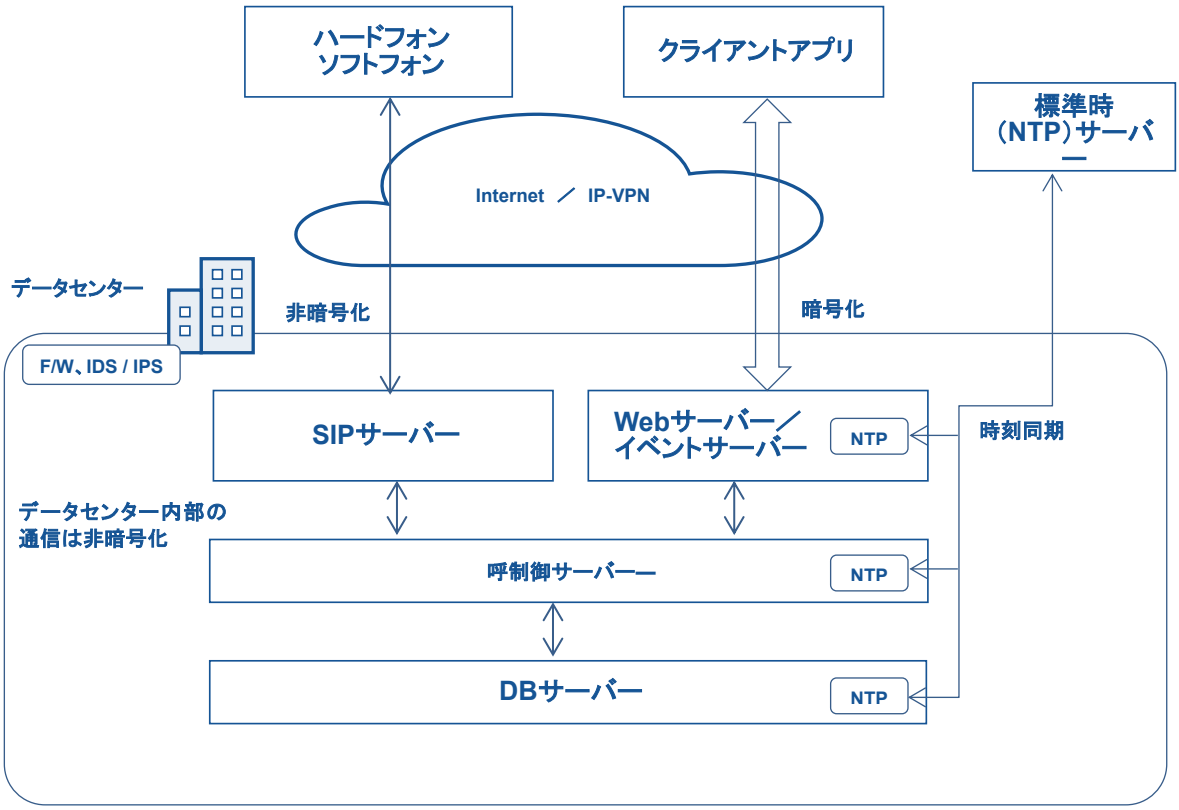
2.1.1 「テナントID」について

各テナントの情報については、テナントごとにユニークな「テナントID」をキーに各種テナントの情報にアクセスするため、テナントに関する情報にアクセスする際、他のテナントの情報が参照されることはございません。



2.2 サーバーセキュリティ

サーバーは、Web／イベント、呼制御、DBの3階層構造となっております。
テナントに関するデータは基本的にDBサーバーに保管され、階層として最下層とすることで情報に対するセキュリティを確保しております。

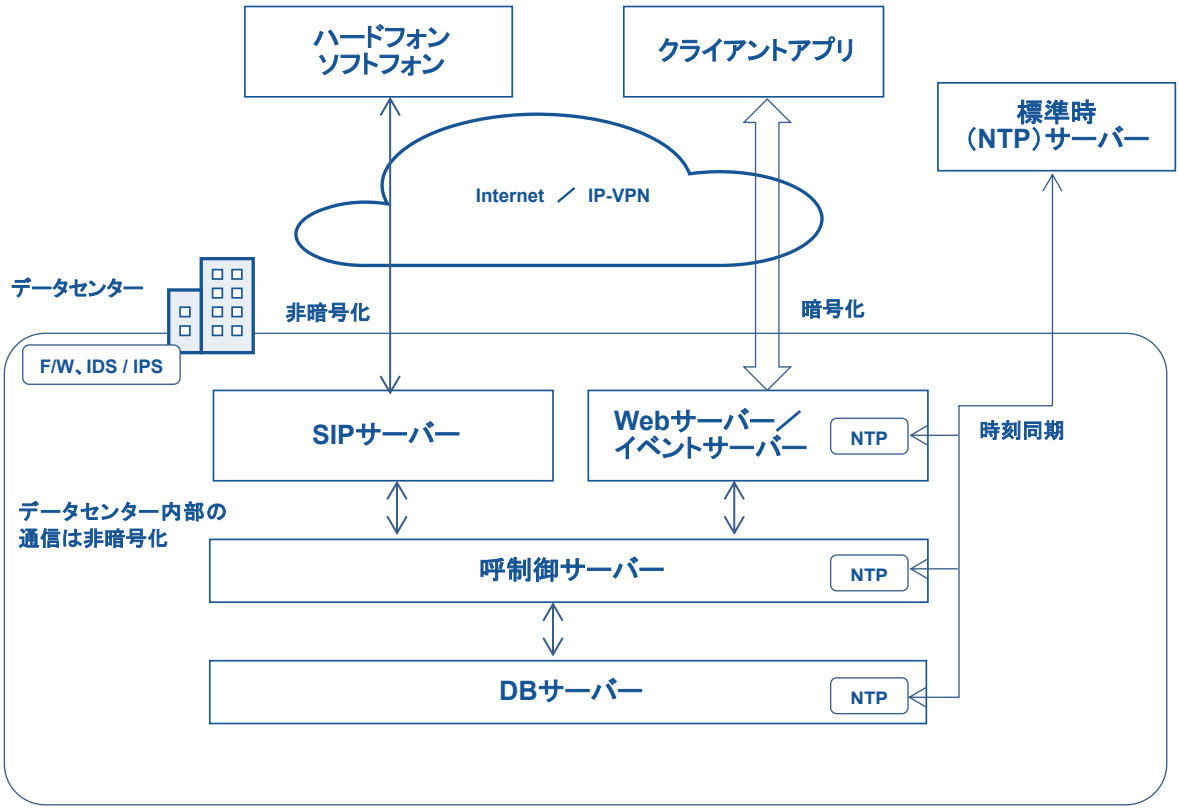


サービス機器については国内のデータセンターに設置されており、他のクラウドサービス（AWS、Azure）は利用しておりません。（標準サービス導入時の場合）
時刻同期についてはNTPサービスを利用して日本標準時（NICT公開NTPサービス）と同期しております。

2.3 ネットワークセキュリティ

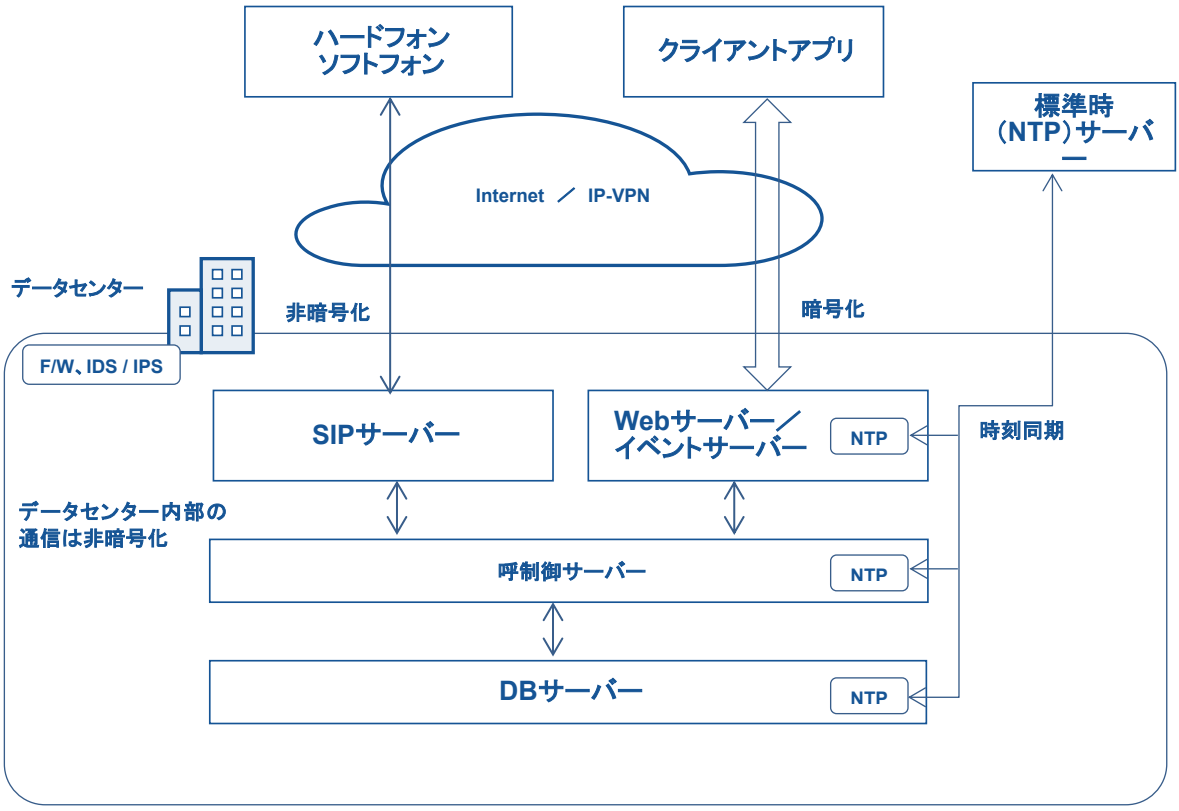
2.3.1 インターネット構成、VPN構成

インターネット経由のアクセス方法と、VPNを利用した閉域網のアクセスのどちらも構成として可能です。
VPN方式としては、IP-VPN／インターネットVPNいずれも利用可能です。
※具体的なFQDN、IPアドレス、ポート番号については「ネットワーク設定書」」をご参照ください。
※VPN構成に必要なサービスについては、お客様手配となります。



2.3.2 データ通信、音声通信

データセンター外部との通信についてはファイアウォール、IPS/IDSを設置しております。
クライアントアプリとサーバー間のデータ通信は暗号化（TLS）しておりますが、音声通信（ソフトフォン、ハードフォンとSIPサーバー間の通信）は暗号化されておりません。
※音声通信の秘匿については、VPNによる閉域網の利用を推奨しております。
また、データセンター内の通信・データ保存については暗号化しておりません。



2.4 クライアントセキュリティ

2.4.1 クライアントのパスワードについて

- ・文字数（任意の文字数指定、標準は8文字）
- ・有効期限（日付指定、標準は期限なし）
- ・リトライ回数の指定（任意の回数指定、標準は無期限）
- ・英語大文字を強制（有効／無効、標準は無効）
- ・英語小文字を強制（有効／無効、標準は無効）
- ・数字（0から9）を強制（有効／無効、標準は無効）
- ・記号（!"#$%&）を強制（有効／無効、標準は無効）

2.4.2 管理者機能

管理者機能（Suite）についてはMACアドレスをご利用いただく形となります（ID・PW認証も可能です）。

2.5 個人情報

CT-e1/SaaSサービス提供において個人情報の考え方について示します。

2.5.1 通話録音ファイル

CT-e1/SaaSサービスでは、通話データを録音しており、再生が可能です。通話録音は、受電時の通話相手の電話番号と対になり保存されます。
弊社の通話録音ファイルは、電話番号と紐づいていますが、それ以外の特定の個人を識別するための情報とは紐づいておりません。よって、個人情報には当たらないとの認識です。
同様の理由から、録音していることについての通知義務は原則不要と考えております。
なお、通話録音ファイルの保存期間は最大3か月間となります。
サービス解約後は原則一ヶ月以内に削除いたします。（お客様へ返却することはございません）

2.5.2 その他のクラウドに保存する情報

CT-e1/SaaSでは、通話履歴等の情報として、クラウド上のサーバーに下記情報を保存します。

① 電話番号（外線番号、内線番号※PSTN（PBX）連携時の携帯番号含む）
② 局番スキル・着信スキルのスキル名
③ エージェント名
④ 顧客利用データ帳票（レポート） ※最大1年間保存

2.6 知的財産権

サービスに関する著作権、商標権等の知的財産権はコムデザインに帰属します。

3 運用の流れ

3.1 問い合わせの流れ

問い合わせは、メールと電話で対応します。

3.1.1 メール

平日9:00～18:00（受付は24時間）

support@comdesign.co.jp

3.1.2 電話

平日9:00～18:00

東京：050-5808-5500

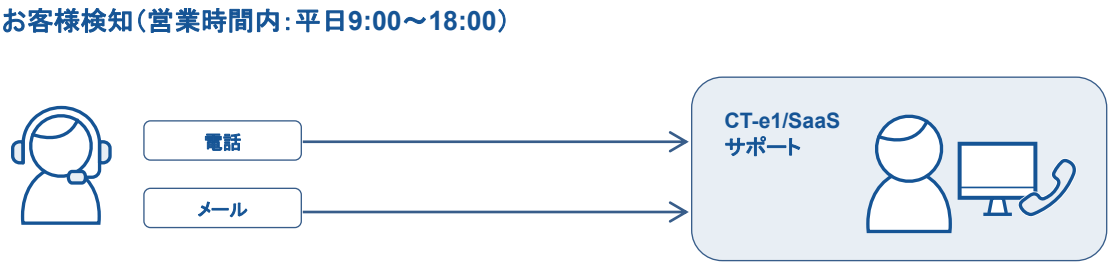
大阪：050-5808-8288

3.2 障害時の流れ

3.2.1 お客様が検知した場合

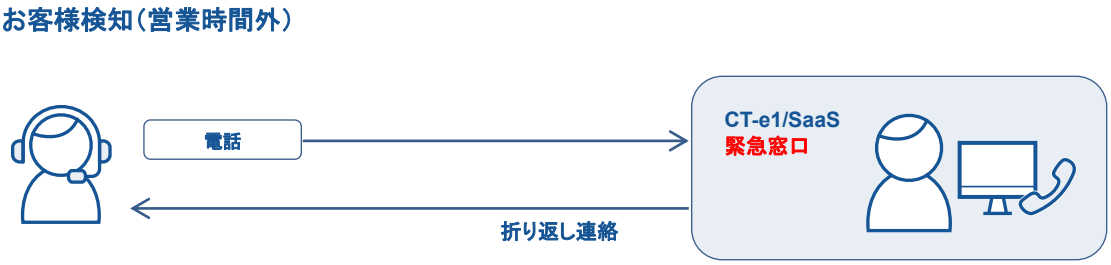
営業時間内（平日9:00～18:00）

電話、メールにて連絡を承ります。



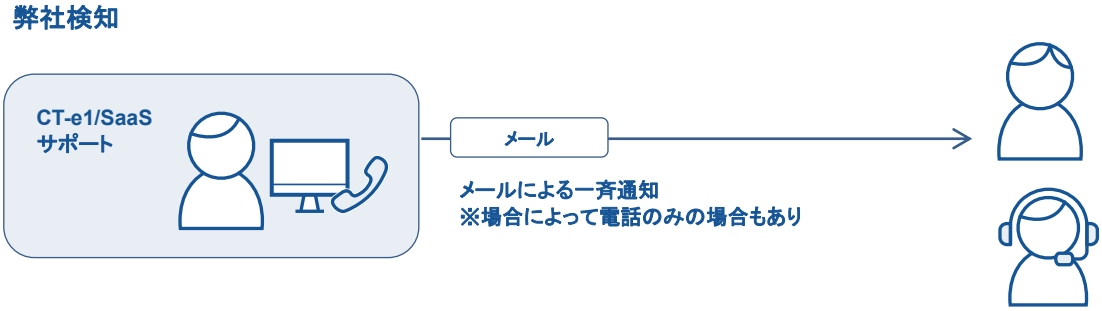
営業時間外

緊急窓口にご連絡いただければ、担当者から折り返します。



3.2.2 弊社が検知した場合

メールにて一斉通知します。※場合によって電話のみの場合もございます。



3.2.3 その他

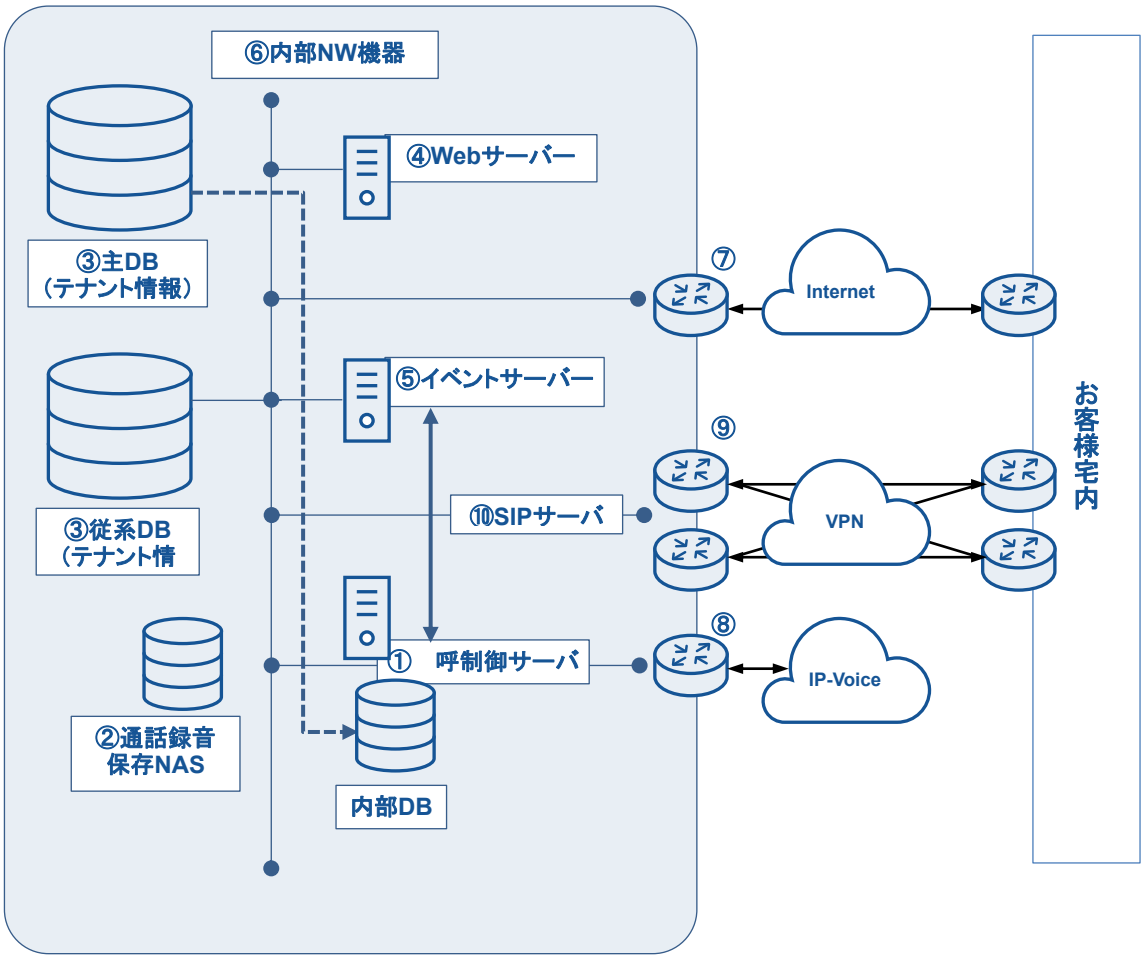
その他、広く情報提供が必要と判断した情報（セキュリティ脆弱性情報等）については必要に応じてホームページへの掲載を行う場合がございます。

4 付録

4.1 障害時切り替え方針影響

4.1.1 CT-e1/SaaSシステム構成概要図

CT-e1/SaaSサービスを提供するデータセンターのシステム構成は下記の通りです。



4.1.2 想定される障害パターン

CT-e1/SaaSにおいて、上記システム構成にて想定される障害パターンごとの対策について説明します。

①呼制御サーバー

典型的なユーザー影響

CTI電話番号に架電しても無音、もしくはビジー切断。発信不可。

障害発生時対応

キャリアサービスによる他電話設備（PBX等）への着信迂回

※故障時の通話呼は切断されます。

障害復旧時対応

コミュニケーターツールの再ログイン、管理者ツールの再起動。

②通話録音保存NAS

典型的なユーザー影響

障害発生時の通話録音ファイル喪失

障害発生時対応

特に不要

障害復旧時対応

特に不要

③DB

典型的なユーザー影響

ログイン不可、一部API利用機能利用不可

障害発生時対応

特に不要（DB切り替えによるサーバー側対応のみ）

障害復旧時対応

特に不要（DB切り戻しによるサーバー側対応のみ）

④Webサーバー

典型的なユーザー影響

ログイン不可、一部API利用機能利用不可

障害発生時対応

通常はアプリケーション側で自動判定・切り替え実施

※強制設定変更は設定ツールによる変更（詳細手順は別途提示）

障害復旧時対応

アプリケーション側で自動判定・切り戻し実施

※強制変更時はツール設定の切り戻し（詳細手順は別途提示）

⑤イベントサーバー、⑥内部NW機器

典型的なユーザー影響

コミュニケーターツールを操作すると固まる。

状態モニタにエージェントの表示がされない。

障害発生時対応

キャリアサービスによる他電話設備（PBX等）への着信迂回。

障害復旧時対応

コミュニケーターツールの再ログイン、管理者ツールの再起動。

⑦インターネット、⑨VPN網

典型的なユーザー影響

コミュニケーターツールが操作できない（勝手にログアウトする、起動しない等）

IP電話機の画面にエラーが表示される。

障害発生時対応

キャリアサービスによる他電話設備（PBX等）への着信迂回。

障害復旧時対応

コミュニケーターツールの再ログイン、管理者ツールの再起動。

IP電話機の再起動

⑧電話網

典型的なユーザー影響

CTI電話番号に架電してもビジー切断、もしくは故障ガイダンスが流れる。

障害発生時対応

キャリアサービスによる他電話設備（PBX等）への着信迂回。

障害復旧時対応

特になし

⑩SIPサーバー

典型的なユーザー影響

着信ポップアップ後、すぐにエージェントツールが後処理になる。

IP電話機の画面にエラーが表示される。

障害発生時対応

コミュニケーターツールの内線に固定電話・携帯電話等の一般電話を設定

障害復旧時対応

IP電話機の再起動

4.2 サービス性能要件

CT-e1/SaaSのサービス性能要件は下記表のとおりです。

種別	標準性能値
同時通話数	200～600件
最大CPH	15,000件
ひと月あたり呼量	300,000件
テナントあたり局番数	150件
CCPあたり局番数	400件
同時ログインOPE数	400件
同時接続管理者数	100件
テナント管理者数（含むActiveBoard）	50件

4.3 セキュリティ要件詳細

CT-e1/SaaSサービスにおけるセキュリティ要件については下記表のとおりです。

適応欄の記号 ○:満たしている ×:満たしていない △:どちらでもない ―:チェック対象外

大分類	分類	チェック内容	適応	回答
基本情報	事業内容	主な事業内容の概要は何なのか。	○	自社開発のオンデマンドコンタクトセンターCTIサービス「CT-e1/SaaS」のSaaS提供になります。
	サービス事業者の信頼性	クラウド事業者の経営状況、市場評価、中長期のロードマップが示されているか。	○	対応しております。
	認証取得	情報セキュリティに関する認証を取得しているか。(ISO/IEC 27001もしくはそれに相当する認証の取得、対策が講じられているか) また、クラウドサービスに関するセキュリティ認証を取得しているか	○	ISO/IEC 27001:2013・JISQ 27001:2014 ISO/IEC 27017:2015 を取得しております。 (ISOの認定登録証写真であれば提供可能です)
		個人情報保護に関する認証を取得しているか。(ISO/IEC 27018もしくはそれに相当する認証の取得、対策が講じられているか)	△	プライバシーマーク等を取得しております。 https://comdesign.co.jp/company/profile/ 但し、原則弊社側での個人情報取得は行いません。
		内部統制に関する監査基準であるSAS70、18号監査、ISAE3402、SSAE16等に適合しているのか。	―	CT-e1/SaaSの提供形式はクラウドサービス(SaaS)のため、お客様の内部統制監査の対象外です。
	利用環境	システムを提供する上で、第三者が提供するシステムを利用しているのか。	×	利用しておりません。自社開発となります。
		CT-e1の動作環境はどのパブリッククラウドとなるのか。	―	すべて自社サービスとなります。 耐震や電力供給等の基準を満たした複数の大手データセンターにて、自社スタッフにて構築されたハードウェア上で展開しております。
		サービス仕様について、責任分界点の明確化、データの取り扱いにおけるポリシーや、リスク対策に係る情報が十分に明記されているか。	○	弊社契約約款をご確認ください。
		サービスの利用可能日、時間はいつなのか。	○	24H365Dになります。
		利用規約等での記載はあるのか。	○	弊社サービス約款は下記に記載のものとなります。 「CT-e1SaaS コンタクトセンターサービス契約約款」 https://comdesign.co.jp/pdf/CD_SRV300.pdf
		システムを利用するにあたり契約上の準拠法と裁判管轄はどこなのか。	―	・準拠法:日本国法 ・裁判管轄:東京地方裁判所
		サービスを利用できる言語が要件を満足しているか。	○	弊社契約約款をご確認ください。
		サービスの可用性(サービス稼働率)は要件を満足しているか。	○	全体稼働率99.999%達成(2020年実績)※SLA上は99.7%となります。
		利用端末環境(OS・ブラウザ・ネットワーク環境等)は要件を満足しているか。	○	端末要件 PC端末推奨スペック NW要件 ネットワーク設定書
		通話の際のネットワーク接続に対して条件はあるのか。	○	IP電話利用の場合には1通話あたり150Kbpsの帯域が必要になります。
		バージョンアップに関する情報取得方法、実施基準、実施間隔は適切なのか。	△	弊社判断により必要に応じて情報提供・実施いたします。
		無料サービスや試行的利用サービスの提供が十分か。	○	トライアル利用サービスを提供しております。
		開始時期、提供組織数、利用者数等市場にて十分な実績があるか。	○	利用社数は1,200社、利用席数は24,000席となります。 (2021年6月時点)
		日本国以外でシステムを利用する場合、システムの利用が制限される国はあるのか。	△	国にもよりますが、条件を満たしているのであれば原則利用回線の仕様に準じた形で発着信は可能です。
		委託業務の有無および委託先数はどのくらいなのか。 また他社に業務を委託するケースはあるのか。	×	委託業務の受託および他社に業務を委託するケースはございません。
		①CT-e1/SaaSの利用はIEコンポーネントの利用が必要 ②CT-e1/SaaSの機能のほとんどは、IEコンポーネント(MSHTML)で実装されており、これはMS社サポートが引き続きあるため、挙動の不具合は起きないと考えられる	○	ご認識の通りです。 ※IEモードを含むIEコンポーネントはマイクロソフトが2029年までサポートしております。
		Edgeで利用できることが理想的だがどうしてもIE11での利用となる場合、何か挙動に不具合はおきないのか。	○	「IEデスクトップアプリケーション」に依存する機能の対応は完了しております。 IEコンポーネント(MSHTML)についてはMicrosoft側から後継コンポーネントが提供されており、そちらへの移行を現在進めている段階でございます。

大分類	分類	チェック内容	適応	回答
	情報管理	利用者データの所在地が要件を満足しているか。また所在地が事業者都合で変更されることがないか。	△	弊社契約のデータセンターにて管理。保管場所について、弊社都合での変更はあり得ます。
		システムリソース不足等による応答速度の低下の検知の場所、検知のインターバル、画面の表示チェック等の検知方法はあるのか。	○	呼処理の応答有無、タイムアウト検出により検知しております。 またシステム保守者にメールにより通知いたします。
		ネットワーク・機器等の増強判断基準または計画の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要はあるのか。	○	ネットワーク機器（スイッチ等）の閾値監視により、閾値超えを検収後、原因特定の上別系への分散にて対応しております。
		定期的な開発・運用者向けセキュリティ教育が実施されているか。	○	ISMSの基準に基づいた対応を行っております。
		貴社内の当該サービスに関わるシステム保守担当者等による情報の持ち出し等の内部不正対策を行っているか。	○	行っております。
		対策を行っている場合どのような内容（組織的・人的・技術的対策）なのか。	○	入社時および通年で教育・セキュリティテスト実施（情報セキュリティ規程（ISMS)にて定義） 社内規程の変更の都度、全従業員に通知し、周知を行っております。
		重要情報が漏洩した場合の補償は明確になっているか。	○	弊社契約約款「第7条（責任および保証の限定）」をご確認ください。
		企業様が入力・保存するデータに対して、弊社による取り扱いがあるのか。	○	通話録音については障害対応等で音声内容を確認するケースがございます。
提供機能	データセンターおよびサーバー状況	サーバールーム（弊社DC）への入館方法はどのような対応が必要なのか。	―	入館責任者：契約先様の中で、あらかじめ弊社に入館責任者を登録いただきます。弊社のシステム経由にて入館希望日をあらかじめ申請いただき、入館できます。 入館責任者以外（※ベンダーだけでなく、契約者の入館責任者以外の方も含む）：　入館責任者から弊社のシステム経由にて入館希望日をあらかじめ申請いただき、入館できます。
		サーバールーム（弊社DC）の記録と保存期間はどのくらいなのか。	―	Logを5年間保存しております。（防犯カメラの稼働時間と監視映像保存期間）
		サーバールーム（弊社DC）の稼働時間はどのくらいなのか。	―	終日になります。（モーションキャプチャー方式（動作検知方式））
		サーバールーム（弊社DC）の保存期間はどのくらいなのか。	―	90日間になります。
		建物（ビル）への入退室方法はどのような対応が必要なのか。※開館時	―	手続きは特に必要ありません。
		建物（ビル）への記録と保存期間はどのくらいなのか。	―	ビル側での管理になります。
		データセンターの立地(国・地域)は要件を満たしているか。	○	東京23区内及び大阪にそれぞれ複数の拠点があります。※JDCC FS（Tier3相当）
		データセンターへの侵入対策はどのように行っているのか。	○	データセンターへの侵入を防止するため、カメラによる監視、生体認証を始めとした高度な認証の実施、入退室ログの取得・管理などを行っております。
		サーバールームへの侵入対策はどのように行っているのか。	○	サーバールームへの侵入を防止するため、各区画のセキュリティレベルに応じた、カメラによる監視、生体認証を始めとした高度な認証の実施、入退室ログの取得・管理などを行っております。
		機器、外部媒体などの盗難対策はどのように行っているのか。	○	上記対策として代替しております。
		サーバー管理者はサーバーに対して運用管理体制を確立し、維持されているか。	○	対応しております。
		サーバー管理者は必要な運用管理業務の手順書を作成しているのか。	○	対応しております。
		サーバー管理者は、サーバーの修理・保守業者との間で業務委託契約におけるNDAを締結しているか。	―	自社内ですべて管理しております。
		サーバー管理者は、保守時にインターネット経由の通信がある場合、暗号化対策等により通信を保護しているか。	○	対応しております。
		サーバー管理者は、保守用に利用する機器にウイルス対策を施しているか。	○	対応しております。
		サーバー管理者は、サーバーに対する保守用に通信について、接続要件に従ったアクセス制限を施しているか。	○	対応しております。
		サーバーの修理・保守作業時は、対象がハードウェア・ソフトウェアに関わらず、休日および夜間含めてサーバー管理者が指名する管理担当者が作業に立会い確認を実施しているか。	○	対応しております。
		サーバー管理者は、サーバー上の不要なアプリケーション機能（サービス）を停止し、不要な通信ポートは閉鎖しているか。	○	対応しております。

大分類	分類	チェック内容	適応	回答
		サーバー管理者は、担当者以外の者が容易にサーバー操作できないような対策を行っているか。	○	対応しております。
		サーバー管理者は、ログに記録する時刻の一貫性を維持する機構を導入し運用しているか。	○	対応しております。
		サーバー管理者は、変更管理手順を文書化し、変更管理手順に従って変更作業の記録を取得・管理しているか。	○	対応しております。
		サーバー管理者は、ログの取得におけるログ管理手順を確立しているか。	○	対応しております。
		サーバー管理者は、ログをどのくらいの期間保存しているか。	―	非公開になります。
		サーバー管理者は、利用者IDを個人に対して発行し、共有利用が無いことを確実にしているか。	○	特権ID利用時は踏み台サーバーに個人IDでアクセスすることで個人認識を実施しております。
		サーバー管理者は、データのバックアップ手順を定め、バックアップの運用体制や周期、媒体保管方法などを定めているか。	○	対応しております。
		データセンターの移設もしくは、既存データセンターの設備が変更される場合には現行相当のセキュリティが担保されるか。	○	現行相当のセキュリティが担保されます。
		安全対策基準（FISC）、もしくは、データセンターファシリティスタンダード（日本データセンター協会）または米国データセンター規格「データセンター用設計規格TIA-942やTIA-942-A」等に準じた物理セキュリティを備えたデータセンターにてサービスが提供されているのか。	○	データファシリティスタンダードのティア3～4に準拠しております。
		インシデントが発生した場合、データセンター等への立ち入り検査や監査に対応しているのか。	△	対応内容によって可否がございます。
		サイトツアー（監査ではないが、データセンター施設の観察）を実施することは可能なのか。	○	可能でございます。
		データセンターで以下のような耐震対策が行われているのか。 例 ○建物、設備、コンピュータ等への影響を防止する措置が講じられていること。（地震による天井・壁・照明器具等の落下・損壊の防止措置、各種機器の床固定、免震床など） ○データセンターが海外にある場合、その所在国において耐震対策について特別に定める法律等がある場合には、それに従った対応を行っていること。	○	行っております。
		データセンターにおける雷対策を教えてください。	○	避雷針、避雷器(サージ防護デバイス：SPD)の設置を行っております。 ※一部データセンターには避雷器の設置はございませんが、電源設備が非接地方式になっており、接地(地面)からのサージ影響は受けません。
	拡張性	カスタマイズの範囲の規定はあるのか。	○	あくまでCTI部分となり、対応可否については要件をすり合わせの上合理的に判断させていただきます。 またカスタマイズ（機能追加）等で費用が発生することはございません。
		連携している外部サービスの範囲は要件を満足しているか。公開されているAPIの範囲は要件を満足しているか。	△	外部サービスの仕様によるため担当ベンダーへご確認ください。
サポート	情報通知	定期報告の内容(監査結果・稼働率実績等)、頻度、方法が適切なのか。	○	最新の情報を記載しております。
		メンテナンス等の告知のタイミングはどのくらいなのか。	―	定期メンテナンスは原則毎月第三木曜日の0:00～7:00となり、原則実施月の第三営業日までにご連絡いたします。 但し緊急な臨時メンテナンスの場合は、直近のご連絡になる可能性があります。
		サービスの一時停止通知方法、タイミングが適切か。	―	緊急連絡先として登録いただくメールアドレスに対し、メンテナンス告知を行います。 当日（臨時メンテナンス）のご案内をするケースもございます。
		有事の際に、以下の資料を提供して貰うことが可能か。 ・有事（情報漏洩・データ改竄）等の調査に必要な資料 ・セキュリティの管理状況に関わる資料	×	他社情報も混在しているため提供不可となります。
	問い合わせ	問合せ窓口(ヘルプデスク)について、下記内容が明確化されており、業務要件に見合っているか。 ①受付時間帯 ②応答時間 ③問合せ可能な範囲 ④手段(メール・電話・チャット)⑤言語	○	①受付時間帯 弊社サービス運用に関する問い合わせおよび変更等：平日9時～18時（弊社定める休日除く） 障害：24/365（上記営業時間外） ②応答時間 ベストエフォート（定め無し）

大分類	分類	チェック内容	適応	回答
				③問合せ可能な範囲 弊社サービスに関する内容 ④手段(メール・電話・チャット) メール、電話 ⑤言語 日本語
	障害対応	障害対応の範囲、内容および通知方法、タイミング、手段が明確で業務要件・運用要件に見合っているか。	○	緊急連絡先として登録いただくメールアドレスに対し、障害報を発報致します。
		通常障害時における平均復旧時間(MTTR)はどのくらいなのか。	―	契約約款(本サービス品質保証)上では原則2時間を超えないことを基準としております。
		通常障害時における目標復旧時間(RTO)はどのくらいなのか。	―	契約約款(本サービス品質保証)上では原則2時間を超えないことを基準としております。
		復旧訓練等を実施し、リストアができることを確認しているのか。	×	検証しておりません。
		重大障害時等に早期復旧が不可能な場合(利用企業側にて他の代替サービスによる運用を開始するための)、バックアップデータの提供は可能なのか。	×	提供はできません。
		過去に発生した障害事例はどのようなのか。	―	非公開です。
		これまでの実績として最長どれくらいの時間サービス停止したか。	―	これまでの実績上、過去5年間で全サービス・全停止はございません。 直近3年間では大規模障害(弊社基準:1/3以上のテナント利用不可)はDB障害30分程度の停止がございました。
	要望対応	要望への連絡手段があり、対応方針が明確化されているか。	○	個別対応とさせていただいております。
情報セキュリティ	情報資産保護	利用者データや派生データに対するクラウド事業者などによる参照や利用(二次利用含む)などが規約などで明確になっているか。 また、その内容が要件を満足しているか。	○	弊社契約約款をご確認ください。
		通信経路は暗号化になっているのか。(HTTPS)	△	インターネットアクセスの場合、下記の通りとなります。 データ経路:SSLによる暗号化対応 音声経路:暗号化なし 必要に応じてVPNによる閉域網による利用も可能です。
		データベースは暗号化されているのか。	×	なっておりません。 現時点では対応不可となります。
		システムにアップロードされるファイルは暗号化されるのか。	×	されておりません。
		データ漏洩・滅失時の補償はされているのか。	○	弊社契約約款をご確認ください。
		多要素認証はされているのか(所有物、生体)。	△	管理者機能についてはMACアドレスによる認証に加えてID/PWを併用可能です。
		SAML認証はされているのか。	×	対応しておりません。
		クラウド事業者の過失や規定違反等によって発生した事象(情報漏洩等)に対する補償範囲や内容が明確になっているか。	○	弊社契約約款をご確認ください。
		・クラウドサービスの機能もしくはOSの機能等を使用し、ハードディスク暗号化を実施しているか。 ・ハードディスク暗号化では、電子政府推奨暗号リストに掲載されている十分安全な暗号化アルゴリズムや鍵長を使用しているか。	△	通話録音データのみオプションサービスとして提供しております。
		・個人情報等の重要情報の取り扱いに際し、データ暗号化は実施しているか。 ・データ暗号化では、電子政府推奨暗号リストに掲載されている十分安全な暗号化アルゴリズムや鍵長を使用しているか。	△	弊社では個人情報等の取り扱いはございません。 また通話録音データのみオプションサービスとして提供しております。
		通話録音データの暗号化費用はどのくらいなのか。	―	以下、概算の参考価格となります。 ■初期(概算) 専用通録サーバー設置作業費　100,000 NAS暗号化設定費用　200,000 ■月額(概算) 専用通録サーバー利用料　100,000
		お客様専用の通話録音サーバーを立てた上で通話録音データをダウンロードする場合、データは復号化された状態でのダウンロードなのか。	×	暗号化はあくまで弊社サーバーへの保存時のみとなります。 ダウンロード時には復号化されます。
		暗号化の桁長はいくつなのか。	―	非公開になります。
		暗号化キーはすべてのテナントに共通なのか。契約するカスタマーごとに異なるのか。	―	非公開になります。
		データベース暗号化の単位は何か(暗号化のアルゴリズムも)。	×	暗号化しておりません。

大分類	分類	チェック内容	適応	回答
		HDDレベルで暗号化を実施しているのか（暗号化のアルゴリズムも）。	×	通話録音ファイルの保存先のみHDDレベルで暗号化可能（オプション） 暗号化方式：AES256
		クラウド事業者独自のバックアップ対策を行っているか、下記について明確なのか。 ・バックアップの対象、範囲 ・バックアップの取得方法、タイミング、保管方法（暗号化の実施状況含）、保存場所（国・地域）、保存期間、世代数 ・データ復元までの時間	○	実施は行っていますが詳細は非公開です
		データのバックアップは行っているのか。	○	対象データや消失タイミングにより異なりますが、最長は1ヵ月、最短は1日の保存期間となります。エージェント情報などテナントのマスタ情報関わる内容については、マスタDBの更新後に各サーバーへレプリケートを行います。対象サーバーの障害時などにはマスタDBから復元を行います。 通話録音データについては、呼制御サーバー側で保存したのちに、ファイルサーバーへの書き込みを行う仕様をとることで導入することでエラー発生時に復元可能です。 ファイルサーバーは筐体間ミラーリングによるデータ二重化済みです。
		以下の内容について、バックアップは取得されているのか。 バックアップ頻度、世代管理を回答してください。 ・業務データ ・プログラム ・ドキュメント（システム設計書、操作手順書、復旧手順書）	○	・業務データ：日次（2世代）、週次：（5世代） ・プログラム：日次（2世代） ドキュメントは対象によって異なりますが複数世代を管理しております。
		重要データについては、サービスレベルに合わせて取得タイミングを定め、遠隔地にバックアップを保管しているのか。	△	遠隔地へのバックアップは未実施となります。
		バックアップを取得する際の情報は暗号化されているか。	×	されておりません。
		バックアップを取得する際の保存期間・世代は指定できるのか。	×	できません。
		システム障害等によりバックアップからデータを戻す場合、どの程度のシステム停止時間が必要となるか。	―	障害の内容・状況によって異なります。
		当該サービスに情報をアップロードする機能はあるのか。	×	対象機能はございません。
		利用者データのバックアップ実施インターバルはどのくらいなのか。	○	設定データ・レプリケートによりリアルタイム、その他データは日時バッチにより退避しております。
		ホストOS、ゲストOS、サーバー、ネットワーク機器、Webアプリケーションなどのログを収集し、セキュリティの確保された環境下で保管（半年以上を推奨）しているのか。	○	一部のログは半年未満（一週間）となります。 またログの提供は致しかねます。
		ホストOSやゲストOSにおいて、不必要なデーモンの停止やサービスアカウントの無効化を行うなどによりサーバーの要塞化を行っているのか。	○	対応しております。
		個人情報の損害賠償保険に加入しているのか。	○	加入しております。
		重要情報を開示するサイトでは、誤情報配信を防ぐ承認フローがあるか。	―	CT-e1では原則重要情報（例：個人情報）の取り扱いはございません。
		ユーザー情報（個人情報）がサービス機能やリスト等を通じて他のユーザーに参照されることはあるのか。	―	CT-e1では原則重要情報（例：個人情報）の取り扱いはございません。
		解約、バックアップ媒体廃棄、データ移行時などの際に、上書き処理や非重要化など重要データが容易に復元できないような仕組みを導入しているのか。	△	廃棄時の物理破壊のみ実施しております。
		情報漏洩や破壊・改ざん等のインシデントが発生した場合に、利用者へ迅速に連絡する手順や体制を確立している。また、緊急時には24時間365日の対応が可能であるのか。	○	可能となります。
		インシデントが発生した場合、該当するログを利用者に提供しているのか。	×	ログの提供は致しかねます。
		企業様が入力するデータは企業様に帰属することになっているか。	○	通話録音データは企業様側に帰属します。
		弊社のサービスの提供に直接必要のある場合（たとえばIDやパスワードの参照、バックアップの取得等）を除き弊社が入力するデータを他の目的への利用（第三者への開示含む二次利用）をしないことになっているか。	○	データの二次利用は実施いたしません。
		企業様が入力するデータをサービスの改善等の目的で貴社のみが参照・利用することがあるか。	○	データの二次利用は実施いたしません。
	アクセス制御	接続元IPアドレス制限はされているのか。 （IPアドレスや電子証明書等による端末接続制限は可能なのか）	×	IPを制限することはできません。

大分類	分類	チェック内容	適応	回答
				弊社アプリケーションがインストールされている機器からのみアクセス可能となります。アプリケーションのインストール対象については貴社にて管理いただきます。 またインストール後、起動時にアクティベーションの為のシリアルコードを入力することで利用可能となります。
		パスワードの設定・管理方法は、情報セキュリティガイドラインに定めるパスワードポリシーに準拠しているか。	○	アプリケーションのパスワードポリシーとして、8文字以上で半角英文字（大文字と小文字）、数字(1文字以上)、記号が利用可能です。
		エージェントIDのパスワードの設定に伴い基準はあるのか。	―	・使用可能な記号 「'」「¥"」「,」「;」「:」「<」「>」「*」「(」「)」以外の英数字と記号 ・設定可能な最小文字数 8文字 ・設定可能な最大文字数 64文字 ※アルファベット数字交じりの8文字以上
		パスワードに関する対策はされているか。	○	弊社アプリケーションからの接続を前提としており、それ以外からのID／PWのアクセスは不可 →改修によりソルト付きハッシュ化を実装いたします。 ※費用はかかりませんが改修に伴いある程度の時間をいただきます。
		パスワードの条件に関して、文字種や文字数以外の条件設定も可能か？	△	現時点では不可能ですが、条件によりますがカスタマイズで対応可能です。
		パスワード有効期限は1年以内か？	○	任意の日数が指定可能です。最大は999日です。
		パスワードの世代管理はされているか？	○	再利用禁止を含めた世代管理を実施しております。世代数は任意で指定可能で、最大は10世代です。
		アカウントロックポリシーは設定されているか？	○	リトライ回数（任意に設定可能）を超えた場合にロックをかけることが可能です。 ロックは管理者ツールで解除可能です。
		ユーザーID（管理者ID・一般ID）の利用について、システムに対して行われた操作は記録されるのか。	○	記録されます。
		アプリケーションへ接続しているログインIDのセッションタイムアウトは何分であるのか。	―	常時接続が前提のシステムのため、該当機能はございません。
		死活監視の対象はあるのか。	○	全体の正常性監視および関連装置の死活になります。
		時刻同期方法はあるのか。	○	Windowsの時間同期になります。
		・管理者や利用者のアカウントや権限(ロール)の仕組みは要件を満たしているか。 ・パスワードについて、下記のポリシーが明確か。(カッコ内は「情報システム利用基準」記載内容) ①長さ(7文字以上) ②複雑性(英字、数字、記号のうち2種類以上) ③世代管理(直近3世代のパスワードは禁止) ④有効期限(半年) ⑤初期パスワード寿命(初回ログイン時に必ず変更) ⑥ロック回数(5回間違いでアカウントロック)	○	①④⑥は対応しております。 それ以外はカスタマイズで対応可能です。
		管理者や利用者のアクセスを制御するために多要素認証や機器固有情報による認証・認可等が実施されているか。	△	管理者機能はMACアドレスおよびID/PW認証が可能です。 エージェント機能に該当機能はございません。
		当該サービスのサーバーでは最低限のサービス・プログラムのみ起動し、不要なプログラムを起動しないようにしているか。	○	対応しております。
		管理用インターフェース（クラウドサービス管理画面）への接続は社内ネットワークからのアクセスに制限する、多要素認証を使用する等の強固なアクセス制御の仕組みを提供しているのか。	○	社内ネットワークからのアクセスのみとなります。
		当該サービスのサーバーにおいて，不要なポートの通信を遮断しているか。	○	対応しております。
		ユーザー単位のアクセス権を設定しているか。(Administratorやrootの管理者権限はサーバー管理者のみに限定)	○	設定しております。
		構築時点で利用可能な修正プログラムは全て適用されているか。	○	適用しております。
		入力系アプリケーションにおいて、プログラムの動作に不都合が生じる特殊記号などのチェックを行っているか。	○	行っております。
		構築時点で利用可能な修正プログラムは全て適用されているか。	○	適用しております。
		サーバーには起動時にパスワード認証がかかるOSとしているか。	○	対応しております。

大分類	分類	チェック内容	適応	回答
		多要素認証に対応しているか。	○	管理者機能のみ対応しております。
		ネットワーク環境から専用線およびVPN等で接続することは可能なのか。	○	可能となります。（別途敷設費用が発生いたします）
		暗号化のための鍵を企業様側の管理者が自身で作成し管理することは可能なのか。	×	できません。
		システムのOSに対するアクセスは、社内NW内からのアクセスに制限されているか。 それとも、外部NWからもシステムのOSにアクセス可能であるか。	○	社内NWからのアクセスに制限されております。
		システムのOSに対するアクセスは、社内NWの中でもセグメント、拠点、フロア等が、制限されているか。	○	本番接続用の端末に制限されております。
		内部ネットワークは冗長化されているのか。	○	しております。
		外部ネットワークは冗長化されているのか。（事業者からインターネットへ接続する回線、または、当社への専用線など）	×	しておりません。
		外部システムと接続する場合はFederated Identity Management（FIM）を使用し、外部システムを認証しているのか。	―	外部システムの接続はございません。
		開発用のシステムIDは、以下のような設定をして使用が制限されているのか。 例 ○本番データやプログラムにアクセスできない設定にしている。 ○本番データやプログラムを、変更、削除できるツールを使用できないようにしている。 （例えばスーパーユーザー機能や強力なユーティリティ等の無効化） ○システム構成情報やネットワーク機器・セキュリティ機器 （例えば、ファイアウォール）にアクセスできないようにしている。	○	開発用のIDと運用用のIDは完全に分離しております。
		システムID貸出時には、ワンタイムパスワードを設定する等の不正アクセス対策を実施しているのか。	―	システムIDの貸し出しは行っておりません。
		以下のIDを利用できるシステム管理者・保守・運用担当者は、限定されているのか。 ・特権ID ・更新権限を持つID ・参照権限を持つID ※OS・DB・MWなどのシステム的なID ※特権ID＝WindowsのAdministratorやUNIXのrootなど、システム上高い権限を割り当てられているユーザーアカウント	○	具体的な利用者人数は非公開となります。
		システムのOSにアクセスできる要員は、一意のID（個人ID）が付与されるのか。 ・特権ID ・更新権限を持つID ・参照権限を持つID	○	特権ID利用時は踏み台サーバーに個人IDでアクセスすることで個人認識を実施しております。
		システムIDは、ワンタイムパスワード貸出が行われているのか。	×	システムIDを利用可能な担当者を限定しております。
	監視・運用	・不正アクセスや管理者等の不正行為の監視(監視内容・間隔)は適切か。 ・不正アクセス等が検知された場合の連絡フローや対応フローは明確になっているか。	○	OS・アプリケーションログのリアルタイム監視を行っております。 検知後のフローについてISMSにて定義しております。
		定期的なアカウントや権限/役割(ロール)の棚卸を実施しているか。	○	年一回実施しております。
		セキュリティ関連ログ(認証含)の取得内容と保存期間は適切か。	△	ログの保存期間は対象ログによって異なります。
		収集したログを定期的に監視し、不正なアクセスや処理等を迅速に検出しているのか。	○	リアルタイムで監視しております。
		・ネットワーク/サーバー/アプリケーションそれぞれの観点でシステム監視基準（監視内容／監視・通知基準）を持っているか。 ・死活監視や主要なプロセスの実行監視をしているか。 ・ネットワークトラフィック量の監視をしているか。 ・レスポンス遅延の監視をしているか。	○	いずれも対応しております。

大分類	分類	チェック内容	適応	回答
		・メモリー、ディスクのリソース監視をしているか。		
		外部ネットワークから内部ネットワークを隠ぺいするため、非武装セグメント(DMZ)を設置しているか。	○	設置しております。
		通信を許可するアプリケーションを必要最小限に限定しているか。(インターネットからクラウド事業者に向けたFTP、TELNET等の悪用可能な通信は、合理的な理由がない限り許可しない。)	○	通信および通話する際にはネットワーク設定やアプリケーションへのログインが必要となります。
		スパム対策サーバーの導入をしているか。	―	サービスとしてのメール受信機能はございません。
		DDoS攻撃を受けた場合に被害の拡大を防止するために、回線業者も含めて以下のような措置を講じているか。 ・攻撃元のIP アドレスの特定と遮断 ・DDoS 攻撃に対して自動的にアクセスを分散させる機能 ・システムの全部または一部の一時的停止 等	○	実施しております。
		利用企業による監査を受け入れることは可能なのか。(目安:年に1回)	○	可能です。 ただし監査内容によっては受入不可の場合もございます。
		以下の場合に、利用企業による監査を受け入れることは可能なのか。 ・官公庁など(金融庁等)の求めがある場合は、調整の上、監査を実施できること。 ・刑事事件や業務委託先起因の情報漏洩等が発生した場合は、調整の上、監査を実施できること。 ・有事(サイバー攻撃等)および、その疑いがある場合は、調整の上、監査を実施できること。	○	可能です。
	サイバー攻撃からの保護	不正侵入やなりすまし対策の仕組み(ファイアウォール/IDS/IPS/WAF設置等による不正侵入防止の仕組み)は導入されているか。	○	F/W、IDS、IPSを導入しております。
		セキュリティ対策の監視等を行っているか(SOC監視等)。 またSOCは内製化なのか外部サービスなのかどちらを利用しているか。	×	未実施となります。
		セキュリティパッチに関する情報取得方法、適用基準、適用間隔(通常、緊急時)は適切なのか。	○	IPAなどの情報セキュリティ機関からの情報を定期的に取得し必要に応じて対応を実施しております。
		ウイルス対策ソフトウェアは導入されているか。また、パターンファイルの更新頻度は適切なのか。	○	インターネットよりアクセスされるサーバーについてははウイルス対策ソフトを導入しております。 またソフト名は非公開となります。
		Webアプリケーション脆弱性対策を実施しているのか。	○	弊社アプリケーションからの接続を前提としており、一般的なWebコンテンツとは構成・内容が大きく異なる(ブラウザから接続してもコンテンツ参照不可) また、URLScanやIIS LockDown 等のツールを利用して、Webアプリケーションのサニタイジングを行っております。 また半期に一回以上の実施ですが、頻度は非公開です。
		Webアプリケーション脆弱性検査診断結果を提出することは可能なの。	○	提出可能です
		OS、M/Wの脆弱性対策を実施しているのか。	○	JPCERT/CC等の最新の脆弱性情報を入手し、新たな脆弱性が発見された場合は必要に応じて対処を実施しております。 また定期的に第三者による外部からの脆弱性診断を行っております。
		脆弱性が見つかることが多いソフト(例えば、WordPressやApache Struts2等)を使用している場合、定常的に脆弱性情報を確認しセキュリティパッチを適用しているか。	×	該当ソフトは利用しておりません。
		企業様が指定する検査機関によるWebアプリケーション脆弱性検査を実施できるのか。	×	クラウドサービスのため企業様指定の脆弱性検査は実施できません。
		不正アクセス対策は実施しているのか。(予防、検知)	○	各種サーバーおよびネットワーク機器の稼働監視、負荷含めた各種リソース監視、不正アクセスに関する監視も実施しております。
		以下のソフトウェアを使用していないこと。 使用がある場合は、その脆弱性のリスクの低減策を回答。 ・Apach Struts	○	使用しておりません。
		当該システムにおいて以下のソフトウェアを使用していないこと。 使用がある場合は、"Flash Player"の使用停止に向けた取り組みを回答。 ・Flash Player	○	使用しておりません。
		監視は何時から何時までが対象時間なのか。	○	24H/365日実施しております。

大分類	分類	チェック内容	適応	回答
		顧客へのサービスに影響が見込まれる攻撃の防御あるいは遮断を行い、顧客データの情報漏洩や破壊などを防ぐための「インシデントに即時対応できる体制」はあるのか。	○	ございます。
		Webサーバーのインシデント対応に必要な連絡機能はあるのか。	○	緊急連絡先への一斉メールによる通知となります。
		「Apache Log4j」の脆弱性を標的とした攻撃について影響もしくはその他懸念事項はあるのか。	―	Apache Log4jについてct-e1ではサーバー・アプリケーションいずれも利用しておりませんので、影響はございません。
サービス継続性	基本方針・計画	事業継続に関する基本方針、計画等は明確なのか。	○	定めております。
		天災、障害等の対応は実施しているのか。	○	サービス対象機器はすべて一定の防災基準を満たしたデータセンターで運用しております。 (1)安定した電源供給 (2)空調設備による適正温度確保 (3)免振対策など また導入後には24時間365日のサポート体制となります。
	代替対策	災害発生時のRTO(目標復旧時間)、RPO(目標復旧時点)、 RLO(目標復旧レベル)が要件を満足しているか。	―	非公開になります。
		DR構成になっているのか。	△	オプションとして対応可能です。
	復旧体制・訓練	災害発生時の復旧体制が定められ、災害復旧訓練が適切な頻度、内容で実施されているか。	―	非公開になります。
契約条件	前提条件	サービス費用に関して、初期費用および月額費用はどのくらいなのか。	○	基本的には「初期費用：¥300,000」「月額費用：1ライセンス¥5,000」になります。 その他細かい部分については構成や利用内容によって異なります。
		下記の契約内容は要件を満足しているか。 ・最短契約期間、違約時の費用の扱い ・契約のバリエーション(年／月／日単位、定額／従量制等) ・プランバリエーション(エコノミー／スタンダード等)	○	最短契約期間は1ヵ月となり、年ではなく月単位でのご契約となります。
	支払方法	支払方法(支払期限・通貨・方法)は要件を満たしているか。	○	当月分の請求内容を末ころに原本もしくはPDFにて送付いたしますので、振り込みにてお支払いください。(手数料が別途発生します)
	解約	利用者からのサービス解約の受付期限があるか。有る場合はその期限は十分なのか。	○	最低解約1ヵ月前までにご連絡ください。
	サービス終了	システムで使用しているハードウェアや記憶媒体を廃棄、またはリース会社へ機器を返却する場合、廃棄・返却作業完了後には廃棄・返却記録が保管されているのか。	○	保存されております。
		第三者に廃棄を委託する場合、第三者と事業者との間で秘密保持契約が締結されるのか。	○	締結されます。
		サービス終了時の通知時期と通知方法は要件を満たしているか。	○	エビデンスメールにてご連絡ください。
		貴社が当該サービスの提供を終了する場合、企業様側ではどのような対応が必要になるのか。	―	弊社から何か依頼することはございません。
		解約時のデータの取り扱いはあるのか。(返却・消去の取り決め)	○	解約時には弊社側で完全に削除します。

4.4 適用法令一覧

適用法令は、下記表のとおりです。

No	法令・ガイドライン名	情報入手先	改正	順守すべき内容（情報セキュリティ関連）	適用管理策等
1	個人情報保護基法 （個人情報の保護に関する法律）	経済産業省 http://www.meti.go.jp/policy/it_policy/privacy/#p20	平29年5月30日 改定	・個人情報の利用目的の特定、利用目的による制限 ・個人情報の適正な取得、利用目的の通知 ・データ内容の正確性の確保 ・従業員、委託先の監督 ・安全管理措置 ・苦情処理等	A.18.1.4 プライバシー及び個人を特定できる情報(PII)の保護 A.5 方針群 （Pマークの運用）
2	東京都個人情報保護条例 （東京都個人情報の保護に関する条例）	東京都 http://www.reiki.metro.tokyo.jp/reiki_honbun/ag1010221 1.html	平31年3月29日 改正		
3	不正競争防止法	経済産業省 http://www.meti.go.jp/policy/economy/chizai/chiteki/	平30年5月30日 改正	・資産の分類・特定、取扱い ・営業秘密の侵害 ・技術的制限手段を解除する製品等の販売 ・信用毀損行為	A.8.2.2 情報のラベル付け A.8.2.3 資産の取扱い A.11.2 入退出管理 A.13.1 侵入防止・検知
4	不正アクセス禁止法	警視庁サイバー犯罪対策 https://www.npa.go.jp/cyber/legislation/	平25年5月31日 改正	・他人のパスワードの無断使用の禁止 ・セキュリティホールを悪用したアタックの禁止 ・別のコンピュータを踏み台とした不正アクセス行為の禁止	A.9.1 アクセス制御
5	著作権法	文化庁、警察庁	平30年7月13日 改定	・著作物、著作人格権の権利の保護 ・ソースプログラム、OS、アプリケーション等の著作権	A.18.1.2 知的財産権
6	電気通信事業法	総務省	令元年5月22日 改正	・電気通信事業者として通信の秘密の順守 ・電気通信事業に従事する間に知り得た他人の秘密の秘匿 ・電気通信番号認定制度への対応⇒認定受領 ・固定電話番号利用についての条件追加への対応 ⇒猶予期間3年　2022年5月21日まで	A.11.2 装置/設備管理 A.12.2 ウイルス検出 A.13.1 ネットワークの保護
7	犯罪収益移転防止法 （犯罪による収益の移転防止に関する法律）	総務省	平30年7月27日 改正	・当社名義の電話番号を顧客の連絡先として使用することを許諾した場合に取引時確認を実施する義務 ・確認記録の作成及び保存する義務 ・疑わしい取引の届出義務	A.18.1.1 適用法令及び契約上の要求事項の特定 A.18.1.3 記録の保護
8	インボイス制度	国税庁	開始令和5年10月1日	適格請求書発行事業者への登録	A.18.1.1 適用法令及び契約上の要求事項の特定