



LLM×RAGを活用した ボイスボットによるCX革新

顧客対応進化とリスク、企業が行うべき運用・対策は？

株式会社ソフトフロントジャパン

代表取締役社長 高須 英司

2025年11月13日

導入① 生成AIが変えるCX：テキスト→チャット→音声



テキスト

FAQ・マニュアル
固定応答



チャット

対話型支援
チャットボット



音声

ボイスボット
AIエージェント

1,016億円

国内生成AI市場（2024年）
IDC Japan予測

145億円

自動対話システム市場（2023年度）
（ボイスボット除く）

122.4→616.9億ドル

グローバル会話型AI市場
（2024→2032年予測）

音声チャネルでも"理解するAI"が一次対応へ

導入② 経営インパクト：生産性・品質・コスト



+30~45%

生産性向上 (McKinsey)



-10%

平均処理時間 (AHT)



+2pt

顧客満足度 (CSAT)



200~400%

ROI (投資対効果)

示唆：コスト削減と顧客満足を同時達成

出典：McKinsey, Gartner, 各社導入事例調査 (2024-2025)



ボイスボット進化① 従来型 vs LLM型

従来型（スクリプト）



固定シナリオ設計

予め定義された分岐パターンに沿って応答。想定外の質問に対応できず、設計・メンテナンスコストが高い。



例外処理の弱さ

シナリオ外の問い合わせでエスカレーション多発。オペレーター負担増、顧客満足度低下のリスク。



手動知識更新

ナレッジ更新には専門スタッフの介入が必須。手間とコストがかかり、最新情報の反映に遅延が生じる。

LLM×RAG型



意図・文脈理解

自然言語の意図を理解し、文脈に沿った柔軟な対話が可能。顧客の真のニーズを把握した応対を実現。



社内ナレッジ安全参照

RAG技術により企業独自の情報を参照し、誤情報（ハルシネーション）を抑制。正確な回答を実現。



高精度音声連携

音声認識精度～95%を実現。自然な会話感覚でのやり取りが可能に。あいまい表現にも対応。

「型にはめる会話」から「意図に合わせて会話を組み立てる」方向に進化

運用影響

更新容易化

拡張性向上

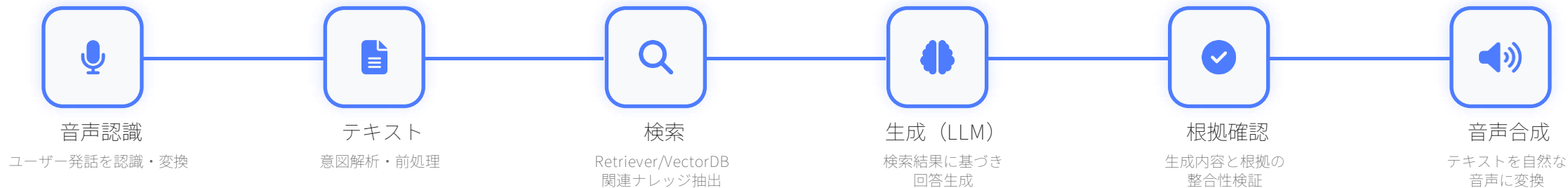
保守性向上

顧客体験向上

ボイスボット進化② LLM×RAG 構成図



「勝手に答えるAI」ではなく「自社の公式情報を参照して正しく答えるAI」に



多層ガードレール設計

入力ガードレール

- PIIフィルタリング
- 有害発言検出・ブロック
- トピック境界判定

生成ガードレール

- システムプロンプト制約
- 権限範囲制御
- 回答形式・トーン規定

出力ガードレール

- ファクト検証
- ポリシー準拠チェック
- 根拠一致検証

RAGの活用で社内ナレッジを安全参照し、根拠に基づく正確な応答を実現

ボイスボット進化③ 意図理解の進化（対話例）



従来型

請求の件で問い合わせています。

お問い合わせありがとうございます。お客様番号をお伺いできますか？

今月の支払いを延ばしたいのですが、可能ですか？

申し訳ありませんが、お客様番号をお伺いできますか？

番号はわからないのですが、支払い期限を延長できますか？

❗ シナリオ外の応答：オペレーターへ転送します

LLM×RAG型

電気代の支払い期限を延ばせますか？

お電話ありがとうございます。お客様の契約番号はA123ですね。今月のご請求の支払い期限は28日となっております。期限の延長は1回につき最大7日間可能です。延長手続きを行いますか？

📖 根拠：支払い期限延長規定 v24.9

はい、お願いします。どのような手続きが必要ですか？

承知しました。特別な手続きは不要です。ただ今、システムにて11月5日まで延長の手続きを完了しました。変更後の期限を記載したメールをご登録アドレスにお送りします。

📖 根拠：延長手続きフロー v3.2

効果

+15%

一次解決率向上

-30%

再問い合わせ削減

+3.2pt

顧客満足度（CSAT）向上



実現例① 段階的導入ステップ

「いきなりすべてをAI化する」のではなく、
「人とAIの役割分担をフェーズごとに設計する」



オペレータ支援

要約・検索・FAQ支援
オペレータの負荷軽減

AHT* -10%



自動応答

時間外/定型手続
特定カテゴリでの自動化

自己解決率 30~50%



統合エージェント

CRM/決済連携
プロアクティブ通知

FCR* +8~12pt

鍵：スモールスタート→継続学習→統合拡張

*AHT：Average Handling Time（平均処理時間）

*FCR：First Call Resolution（初回解決率）

実現例② 事例スナップ（金融／公共／エネルギー）



金融

自治体

エネルギー



「人がいない」という話ではなく、
「人が必要な場面に人を集中させる」という起点発想

口座照会の自動化および延滞相談の一次受付をボイスボットが担当。24時間対応により顧客満足度が向上し、オペレーターはより複雑な相談に集中。

成果

- 🕒 応答時間 -35%
- 😊 顧客満足度 +2.5pt
- 💬 オペレーター高度対応案件率 +22%



証明書発行手続きの案内と粗大ごみ収集予約の受付をボイスボットが対応。庁舎閉館後も住民サービスを提供し、窓口業務の負担を軽減。

成果

- 🌙 夜間応答率 0→100%
- 👥 窓口負荷 -25%
- 📅 住民サービス時間 +128時間/月



料金照会、支払い期限延長、契約変更受付などをボイスボットが自動処理。顧客自身での解決率向上により、問い合わせ対応コストが削減。

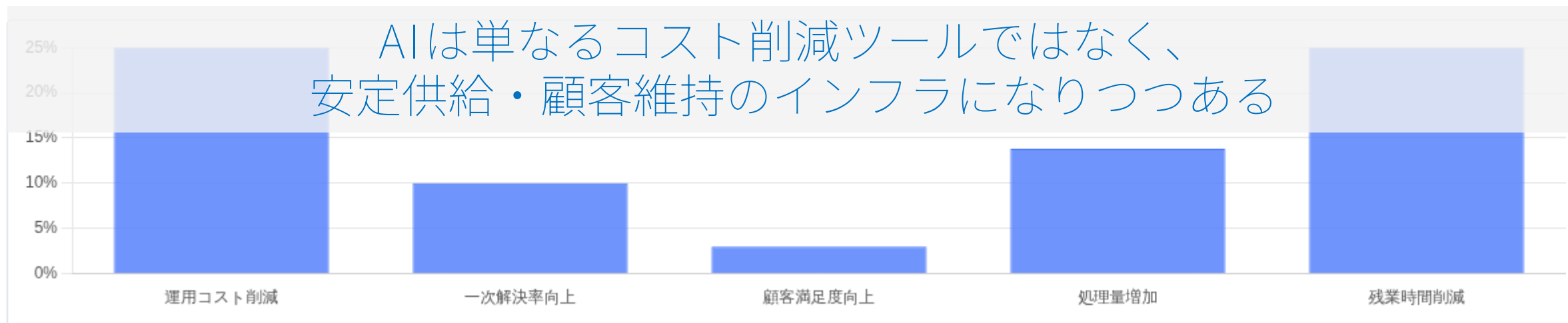
成果

- ✅ 自己解決率 48%
- 🎧 一次解決率 +10pt
- 📞 オペレーター転送率 -32%

実現例③ 効果サマリー（定量）



AIは単なるコスト削減ツールではなく、
安定供給・顧客維持のインフラになりつつある



-20~30%

運用コスト削減



+8~12pt

一次解決率（FCR）



+13.8%

オペレータ処理量



-2h/日

残業時間削減

拡張性：ピーク時のスケールアウト、夜間・休日対応も自動化で継続的なサービス提供を実現

出典：ミック経済研究所、McKinsey、各社公開事例（2024-2025）

課題とリスク① リスク分類

「どの層のリスクなのか？」
を切り分けておくこと



技術リスク

ハルシネーション（幻覚）
誤推論
モデルドリフト

高影響度



データリスク

古いナレッジ参照
権利情報混入
機密情報混入

高影響度



セキュリティリスク

個人情報漏えい（PII）
越権API呼出し
プロンプトインジェクション

高影響度



コンプライアンスリスク

記録義務違反
説明責任不全
業法規制抵触

中影響度



オペレーションリスク

エスカレーション遅延
人的監督不足
体制不備

中影響度



ビジネスリスク

顧客信頼喪失
風評被害
コスト増加

中影響度

リスク対策には技術・プロセス・組織の三位一体アプローチが必要

出典：生成AI導入企業調査（2025）、業界ベストプラクティス

課題とリスク② 誤応答事例（イメージ）



事例と影響



料金計算条件の誤解

特殊割引条件を見落とし、標準料金で請求案内。顧客の事情（高齢者減免など）を考慮せず誤った金額を提示。



潜在的な損害リスク

顧客の経済的損失、信頼関係の毀損、クレーム増加によるブランド棄損、最悪の場合は法的責任問題へ発展。

誤応答シナリオ例

高齢者世帯なんですが、電気代の割引はありますか？

標準料金プランでは、月額5,200円からご利用いただけます。誤情報

高齢者向け割引はないのですか？

申し訳ありませんが、年齢による割引は提供しておりません。誤情報

対策



RAGによる根拠限定

信頼性の高い社内ドキュメントのみを情報源として使用。最新の料金体系・特別割引条件を含むベクトルDB構築と定期更新体制。



重要トピックの出力検証

料金案内、契約条件など重要事項は自動ルールチェックを実施。パターンマッチング＋事前学習済みテストケースによる精度担保。



境界ケースの人間連携

複雑な条件や高リスクトピック（料金体系変更、特別割引など）は自動検知して遮断。オペレーターへのリアルタイム転送体制を整備。

リスク軽減のポイント



多層ガードレール



定期的なナレッジ更新



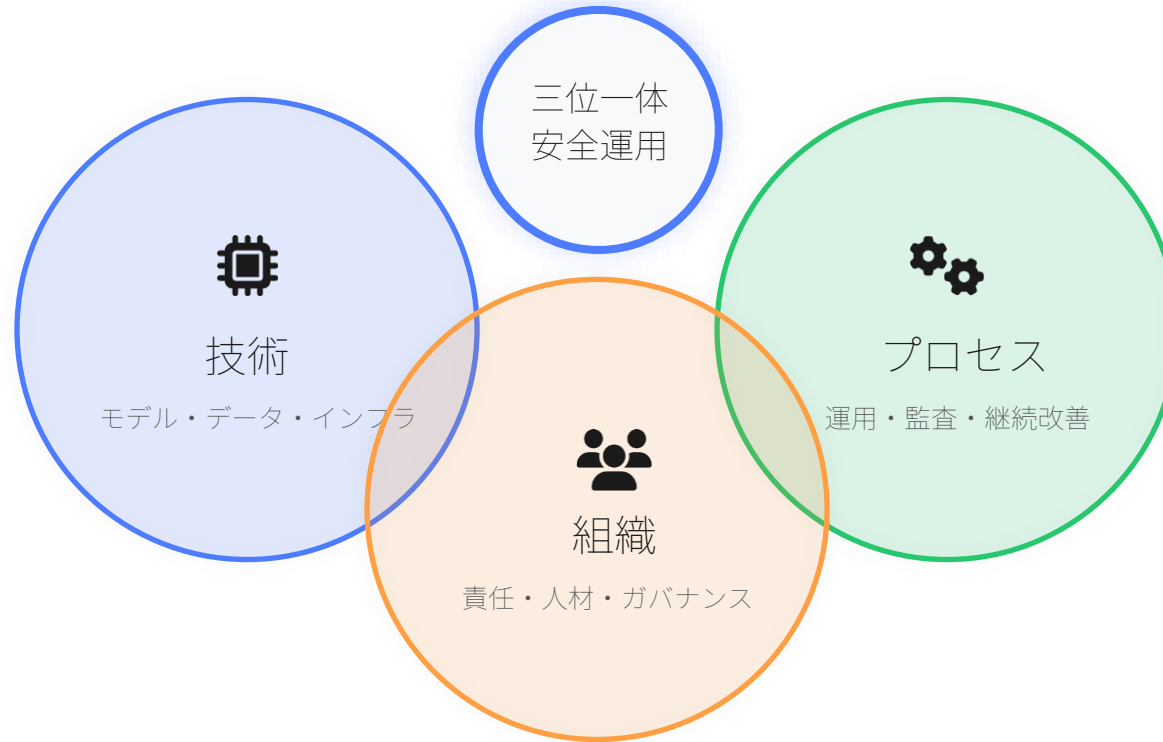
AI応答の監査体制



インシデント早期報告



課題とリスク③ 技術だけでは防げない領域



安全運用に必要な要件

権限分掌役割と責任の明確化承認フロー
の設計

変更管理更新プロセス標準化リリース判
定基準

障害復旧インシデント対応計画緊急停止
・切替手順

定期監査四半期レビュー対話品質・法令
遵守

原則：人間の最終責任・説明可能性の担保

安全運用① 多層ガードレール設計



“全工程で守る”運用設計が重要
AIベンダーとの連携協力も非常に重要



入力層

PIIフィルタ

暴言検出

越権意図検知

ボイスバイオ対策



検索層

ソース信頼度スコア

チャンク品質管理

検索範囲制限

最新性検証



生成層

システムプロンプト制約

ツール使用制御

トーン規範

文脈保持ルール



出力層

ファクト検証

ポリシーチェック

ブロック/訂正

根拠整合性確認



監査

監査ログ

アラート

A/Bテスト

人的レビュー

多層防御による安全性確保：誤答・リスクを全工程で検出・遮断・記録

安全運用② RAG検証フローと評価指標



検索
Retrieval



生成
Generation



根拠確認
Verification



ユーザー提示
Response



フィードバック
Feedback

オフライン評価指標



Context Precision/Recall
検索文書の適合性・網羅性



Faithfulness (忠実度)
回答が検索結果に忠実か



Answer Accuracy
回答の正確性

オンライン評価指標



正答率
目標 $\geq 85\%$



誤応答率
目標 $\leq 2\%$



更新TAT*
目標 ≤ 48 時間

評価の自動化と人的監査の併用がRAG品質維持の鍵

「AIを入れて満足」ではなく、
「AIの品質を継続的に測る」という運用

*TAT: Turnaround Time (処理時間)

安全運用③ ガバナンス体制（RACI例）



責任分担マトリックス（RACI）

役割/プロセス	変更審査	リリース判定	モニタリング	インシデント
運用責任者	A	A	C	A
データ管理者	R	R	R	R
セキュリティ担当	C	C	C	R
法務/監査	C	I	I	C
現場運用	R	C	R	R

RACI（レイシー） 凡例

R: 実行責任者 (Responsible) A: 説明責任者 (Accountable) C: 相談先 (Consulted) I: 報告先 (Informed)

ガバナンス会議体



週次運用会議

参加者：管理者、現場運用担当者
議題：運用指標レビュー、ユーザーフィードバック分析、短期課題対応



月次品質会議

参加者：運用責任者、データ管理者、運用担当者
議題：KPI達成状況、誤応答分析、改善施策立案



四半期監査

参加者：全担当者（セキュリティ、法務含む）
議題：リスク評価、コンプライアンス確認、モデル更新計画



インシデント対応

発生時即時招集
参加者：運用責任者、データ管理者、セキュリティ担当者
対応：状況把握、影響範囲特定、対処方針決定

AIを業務の中核システムとして扱える体制



導入の勘所① ロードマップ（0-12ヶ月）

急がず、でも止まらずに進める

0ヶ月

3ヶ月

6ヶ月

12ヶ月



Phase 1：PoC

ユースケース選定：頻度×難易度×リスクで評価
正答率検証：QAペア、ナレッジマッピング
CSAT・トーン評価：顧客の受容度を確認
技術検証：応答時間・レイテンシ測定



Phase 2：パイロット

限定範囲展開：夜間/特定カテゴリ対応
ガードレール有効性レビュー：誤応答率≤2%
オペレーター連携：エスカレーションフロー確立
改善サイクル：週次改善・ナレッジ更新



Phase 3：本番拡張

CRM/システム連携：顧客情報活用・API連携
監査指標運用：KPIダッシュボード確立
教育・定着化：現場オペレーション改革
機能拡張：システムアップデート、機能追加

鍵：人⇄AIの最適なハンドオフを設計し、ステップバイステップで拡張する

導入の勘所② KPIダッシュボード例



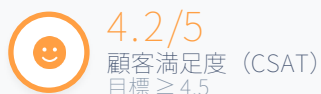
精度



運用



顧客



この運用リズムが「改善されるAI」を具体化する

※ ダッシュボードは部門横断で共有、週次で評価、月次で改善策実施



導入の勘所③ 成功要因（KSF）チェックリスト



経営コミット & 明確なROI目標

トップマネジメントの理解・支援を確保し、**投資対効果（200～400%）**の明確な目標値と達成期限を設定する。



優先ユースケース選定

頻度×難易度×リスクのマトリックスで評価。
初期は定型問合せや時間外対応など、効果が明確な領域から着手する。



高品質ナレッジ整備

RAGの基盤となる**体系的なナレッジベース**を構築。
適切なタグ付けと定期的な更新プロセスを確立する。



多層ガードレールと評価自動化

入力・検索・生成・出力の**各層でのガードレール**反映。
正答率・誤答率の自動評価と継続的改善サイクルを構築する。



スモールスタート→反復改善→段階展開

小規模PoCから始め、**データに基づく改善**を繰り返した上で、範囲・規模を段階的に拡大する展開戦略とする。



現場教育・オペレーション設計

運用担当者向けの**RACI責任分担**と対応手順の明確化。
インシデント対応プロセスと定期的なトレーニングを実施する。

「人をAIに置き換える」発想ではなく、
「人が一番価値を出せる場面に集中できるようにする」という発想

実践ポイント：ユーザー視点と運用視点のバランスが鍵。技術導入だけでなく、組織・プロセス・教育を含めた総合的な取り組みが成功への近道。

まとめ・Q&A／お問い合わせ



💡Takeaway 3点

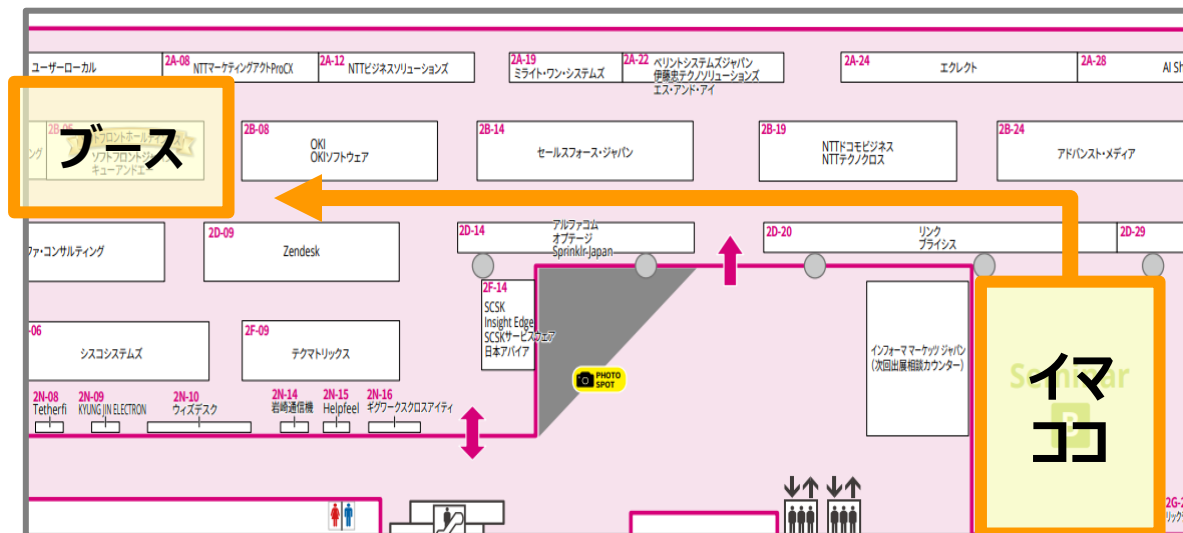
1 LLM×RAGはCX革新の中核。音声一次対応が実用段階

2 安全運用はRAG+多層ガードレール+ガバナンスが鍵

3 段階導入でROIを早期に可視化し全社展開へ

? ご質問をどうぞ

ソフトフロント ブース出展場所
小間番号：2B-5



株式会社ソフトフロントジャパン

Email: sales@softfront-japan.co.jp

Web: <https://commubo.com/>