

だんだん動物園

入場システム テスト設計書 v3.6

*Human Impact*をFMEAに変換した、KGI起点テストアーキテクチャ設計

KGI : 入場トラブル件数 0件/日

2026年版変更対応 : 残数上限60人・パラメータ可変 (V03) ・ゲートハブ継承

00 テストアーキテクチャ概要 — レベル・技法・スコープ

本設計書が採用するテストの全体像。テストレベル・技法・スコープを明示し、判断根拠を透明化する。

📁 テストレベル

ST システムテスト（主軸）

入場フロー全体・ゲートハブ連携・QR認証エンドツーエンド

IT 結合テスト

ゲートハブ ↔ 入場管理 ↔ 発券機間の通信・データ整合

NFT 非機能テスト

性能（≤1秒）・可用性（警告ブザー≤30秒）・整合性（インジケータ反映≤10秒）

🔧 テスト技法

境界値分析

残数(0/1/10)・時間枠境界・ACK回数(3回)

→ TC-201, TC-CAP-01, TC-N04

同値分割

有効QR / 使用済みQR / 無効QR の3分類

→ TC-101, TC-102

状態遷移テスト

Ticket状態:
UNUSED→USED→ENTRY_DENIED

→ TC-102

競合テスト

Web×発券機の同時購入・3ゲート同時スキャン

→ TC-201, TC-N02

📋 テストスコープ

対象

- ・入場ゲートQR認証（ハブ経由・継承）
- ・ゲートハブ集中管理・縮退運転
- ・時間枠残数管理・重複販売防止
- ・入場券情報同期（VPN-GW経由）
- ・非機能：性能・可用性・整合性

対象外

- ・決済システム内部（保証済み）
- ・会員登録・変更・退会
- ・全入力値組合せの網羅
- ・UIデザイン・文言の確認

単体テスト（QR生成・販売ロジック）は開発会社保証済みのためスコープ外。テスト資源をリスク上位に集中させる。

0X 仕様書への問題指摘と設計提案 — 能動的なQA活動

テスト設計の過程で仕様の曖昧さを発見し、フェイルセーフ仕様をこちらから定義・提案した。

SPEC-01

深刻度：重大

ゲートハブ停止時の挙動が未定義

F-01 RPN=96

📄 仕様の問題

仕様書には「ハブ停止時はエラーログを記録する」とのみ記載。
ゲート3台がどう振る舞うか（即時停止 / 縮退運転 / フェイルオープン）が未定義。

⚠️ リスク

フェイルオープン（ゲートが開きっぱなし）になった場合、無制限入場が発生し安全基準違反となる。

✅ 設計提案

「ACK欠如3回連続でフェイルセーフ停止（閉門）し、コンソールにエラー通知・警告ブザー鳴動」を設計として定義・提案。

SPEC-02

深刻度：重大

残数=0と残数=1の同時購入時の排他制御が不明確

F-02 RPN=108

📄 仕様の問題

仕様書には「残数0で販売停止」とのみ記載。
Web・発券機3台が同時にアクセスした場合の排他制御の実装方針が不明。

⚠️ リスク

楽観ロック未実装の場合、残数1の枠に複数購入が成立し重複販売が発生する。

✅ 設計提案

「残数更新時に楽観ロック（バージョン番号チェック）を適用し、競合時は後発リクエストをエラー返却する」を不変条件として定義。

SPEC-03

深刻度：中

VPN-GW切断時の入場管理の継続動作が未規定

F-03 RPN=96

📄 仕様の問題

仕様書には「VPN-GW経由でWebチケットシステムと連携」とのみ記載。
VPN切断中の動作モード（停止 / キャッシュ継続）が未定義。

⚠️ リスク

切断と同時に全入場判定が不能になると、購入済み来園者が入場できない事態が発生する。

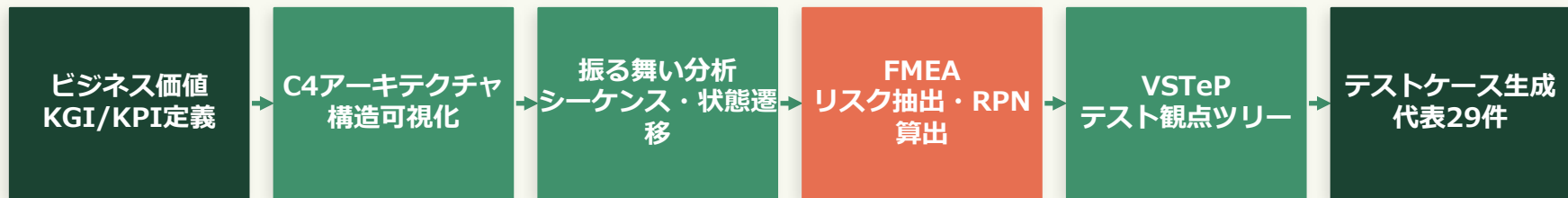
✅ 設計提案

「切断中は既取得の入場券情報キャッシュで継続動作。復旧後は滞留なく速やかに差分同期を完了する」を非機能要件として提案。

仕様の曖昧さを発見し「テスト可能な仕様」として定義することも、テスト設計者の責務である。3件ともFMEA高優先以上のリスクと対応（F-02は最高優先）。

01 設計思想：アーキテクチャ起点テスト設計

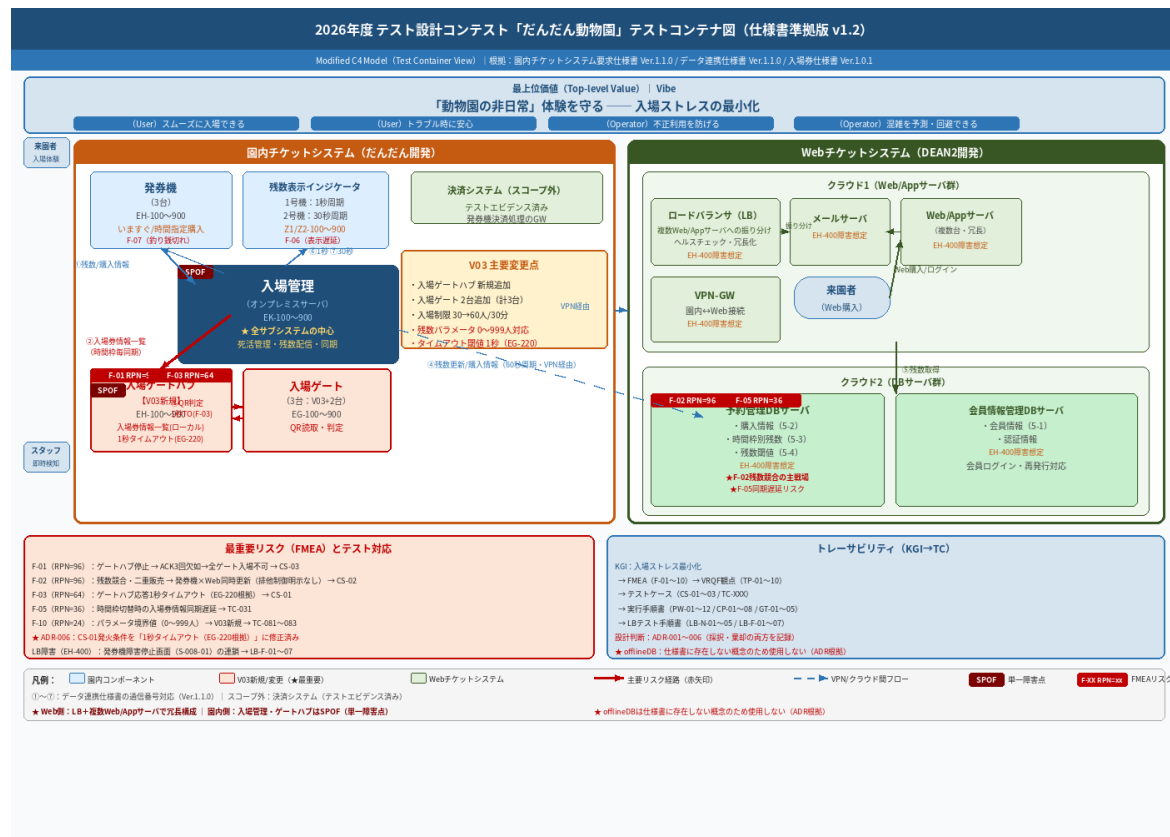
「ビジネス → アーキテクチャ → リスク → テスト」を一本の線で繋ぐ。KGI起点の設計思想。



⚡ 2025年版の核心変更 — なぜこのテスト設計が必要か

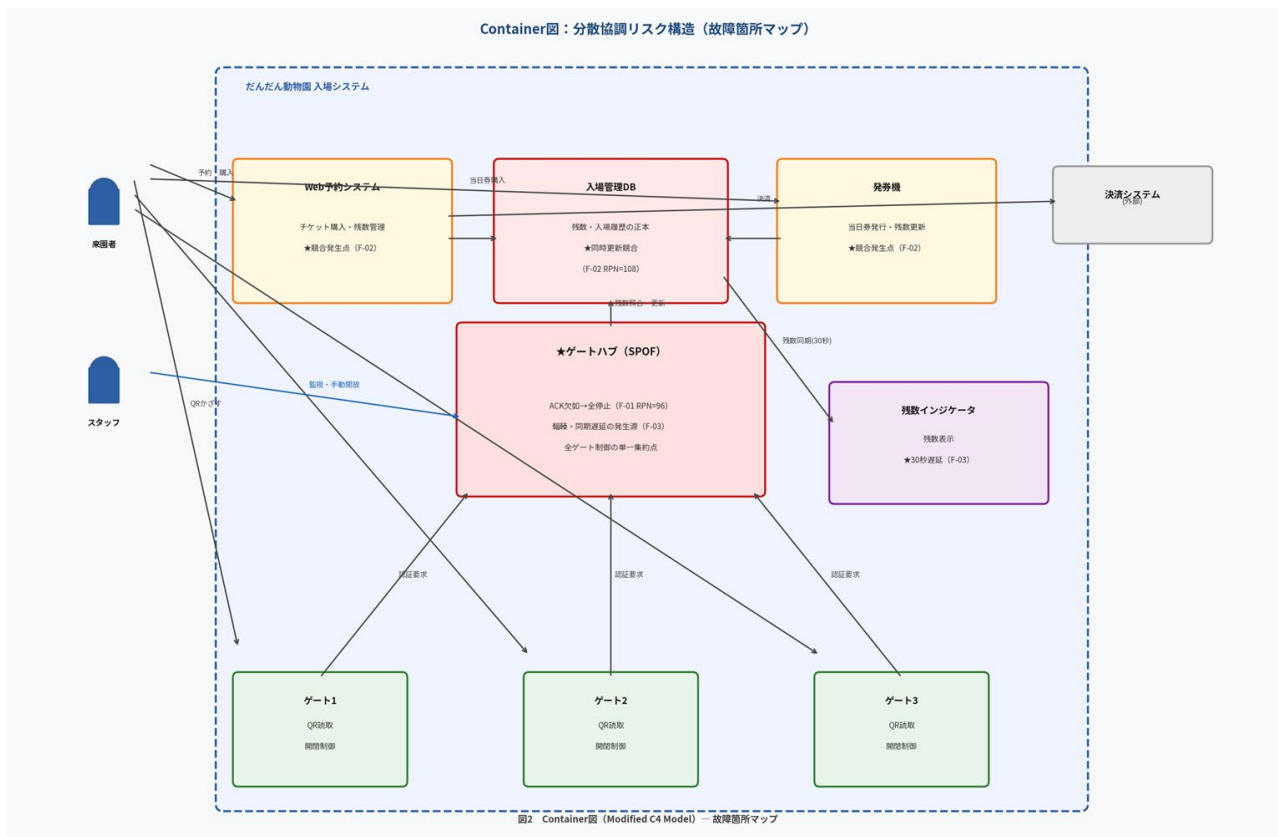
変更前 (2024) :	ゲート直結通信 (1台)	新たなリスク② :	残数同時更新の競合 → 重複販売
変更後 (2025) :	ゲートハブ経由・集中管理 (3台)	新たなリスク③ :	入場券情報一覧の同期遅延・欠落
新たなリスク① :	ハブ停止 → 全ゲート同時不能 (SPOF)		

図1 テストコンテナ図 (Modified C4 Model)



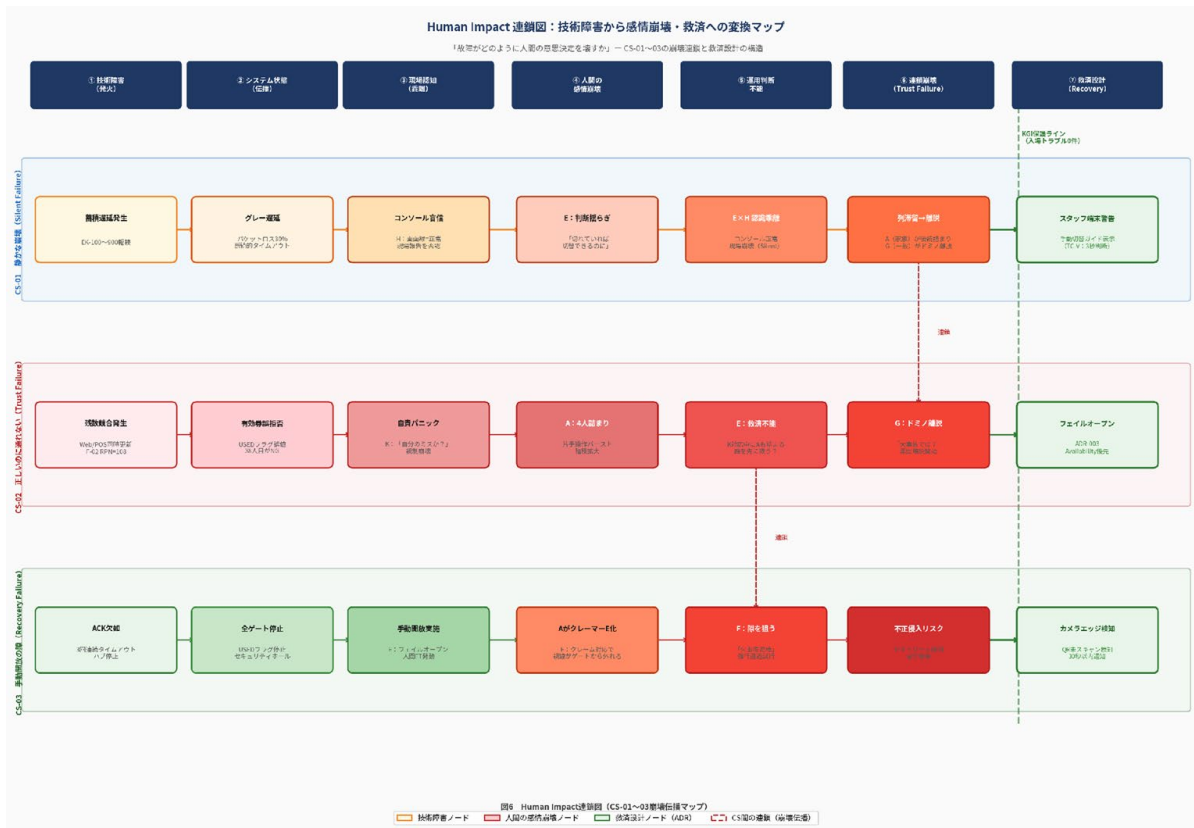
アーキテクチャ起点テスト設計の出発点となるC4コンテナ図 (仕様書準拠版)。第1章に掲載。

図2 分散協調リスク構造（C4 Container Model）



ゲートハブを中心とした、ゲート・入場管理・発券機間の分散協調リスク構造。第4章冒頭に掲載。

図3 Human Impact 連鎖図 – 技術障害から感情崩壊・救済設計への変換マップ



横軸：技術障害→現場認知→感情崩壊→判断不能→連鎖崩壊→救済設計 / 縦軸：CS-01（青）/CS-02（赤）/CS-03（緑） / 右端KGI保護ラインで救済設計が連鎖を止める

02 FMEA — 故障モード影響分析（実RPN値）

S=重大度(1-10) O=発生頻度(1-5) D=検出難度(1-5) $RPN=S \times O \times D$ | 100以上→最高優先 60-99→高優先 40-59→中優先 39以下→低優先

ID	機能	故障モード	ビジネス影響	S	O	D	RPN	優先度
F-01	入場ゲートハブ	ハブ停止→全ゲート同時不能	来園者全員が入場不可・パニック発生	8	3	4	96	高優先
F-02	残数管理	同時購入による残数競合	重複販売→入場拒否で来園者トラブル	9	4	3	108	最高
F-03	情報同期	入場券情報の同期遅延・欠落	有効券が無効判定→スタッフ手動確認	8	4	3	96	高優先
F-04	QRセンサー	センサー故障→単一ゲート機能停止	単ゲート停止・ハブ経由の縮退動作	5	2	3	30	低
F-05	DBサーバ	DBサーバ停止	全機能停止・入場不可・データ消失リスク	9	1	3	27	低

※D値根拠：F-01はACK欠如3回判定まで3秒、来園者への影響が見えにくい。F-03は遅延が正常完了扱いになるケースがある。V03新規：F-CAP-01（RPN=81）残数上限60人超過販売、F-CAP-02（RPN=64）パラメータ0設定時全販売停止、F-CAP-03（RPN=36）パラメータ999制御不能。

03 VRQF優先度指標 — 定義・重み・算出根拠

なぜRPNだけでは不十分か：FMEAは物理的故障リスクを測るが、ビジネス価値や頻度は測れない。VRQFで補完する。

優先度スコア = $(V \times 2) + (R \times 3) + (Q \times 1) + (F \times 1)$ 18点以上 → 高優先 12~17点 → 中 11点以下 → 低

V

Value（ビジネス価値影響）

重み ×2

このリスクが顕在化したとき、KGI（入場トラブル0件/日）への影響がどれほど大きいのか

- ▶ ビジネス価値を守ることが設計の大前提のため

R

Risk（リスク発生確率）

重み ×3

アーキテクチャ・運用条件を踏まえ、このリスクが実際に発生する蓋然性

- ▶ 事故を未然に防ぐことが最優先のため最大重みを付与

Q

Quality（品質影響）

重み ×1

発生した場合のシステム品質（可用性・整合性・性能）への劣化度合い

- ▶ 主軸（R・V）を歪めない補助軸として設定

F

Frequency（発生頻度）

重み ×1

通常運用でこの状況が発生する頻度・条件の起こりやすさ（FMEAのO値と相関）

- ▶ Qと同じく補助軸。Q/Fが高くてR/Vが低い観点を過剰優先しない

VRQFはFMEA（物理リスク）を補完するビジネス・ユーザ視点の優先度指標。両者を組み合わせることでテストリソースを最適配分する。

04 Human Impact Hypothesis → テストケース3例

「壊れたときの顔」→ FMEA → TC。異常系・正常系・境界値の3パターンで設計を証明する。

TC-ID	種別	前提条件	操作手順	期待結果	VRQF
TC-401 HIシート①対応 F-01 RPN=96	異常系	ゲートハブ正常稼働中・ゲート3台稼働中	①ハブをシャットダウン ②コンソール画面を確認	ACK欠如3回検出から30秒以内にコンソール異常通知・警告ブザー鳴動	28点 (高優先)
TC-101 Happy Path 正常フロー (TP-01・継承)	正常系	ゲートハブ正常稼働・有効QR（未使用・時間枠内）	①来園者がQRを提示 ②ゲートでスキャン	ゲート開・ブザー・ランプ点灯。使用済フラグが立つ	31点 (高優先)
TC-201 F-02 RPN=108 残数境界値(0/1)テスト	境界値	時間枠残数=1、WebとPOS（発券機）から同時購入（差100ms以内）	①2チャネルから同時に残数=1の枠を購入 ②両方の購入結果を確認	一方のみ購入成功、もう一方はエラー（残数0）。二重販売なし	30点 (高優先)
3パターン（異常系・正常系・境界値）でTP-01・TP-02・TP-04の主要リスクを網羅。代表ケースのうち3件を抜粋。V03新規：TP-CAPに て残数上限60人・パラメータ境界値テストを追加。					

05 VRQF優先度 × VSTeP テスト観点ツリー

スコア = (V×2)+(R×3)+(Q×1)+(F×1) | 18点以上→高優先 12～17→中 11以下→低

VRQF スコア上位観点

観点ID	観点名	V	R	スコア
TP-01	入場ゲートQR認証	5	5	31
TP-02	時間枠重複販売防止	5	5	30
TP-CAP	残数上限・パラメータ境界値	5	5	30
TP-04	ゲートハブ障害・縮退運転	5	5	28
TP-03	入場券情報一覧同期	4	5	27

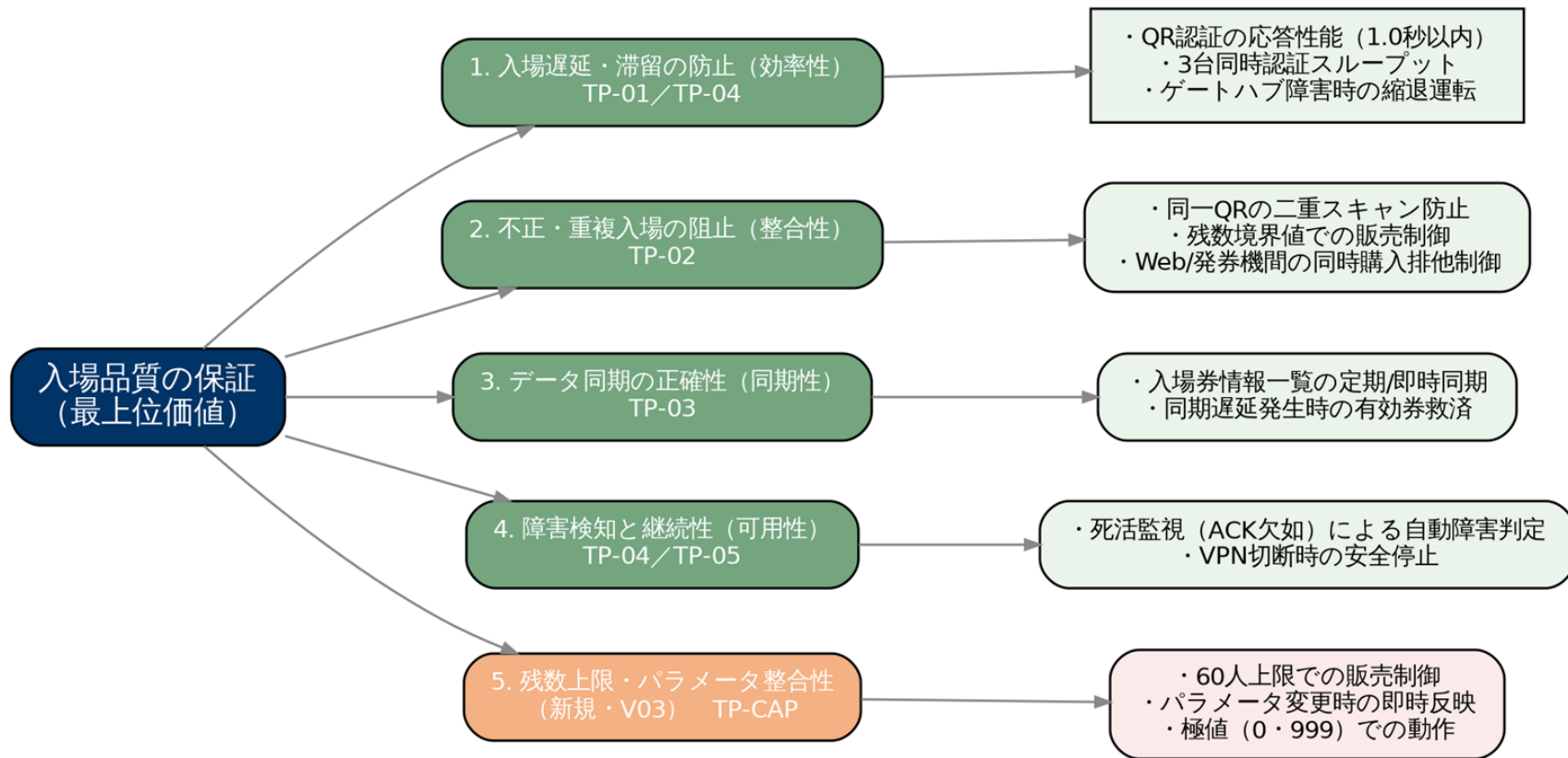
VSTeP テスト観点ツリー

入場品質の保証（最上位価値）

- ▶ 1. 入場遅延・滞留防止（効率性）
 - ・QR認証 1秒以内 / 3台同時スループット
 - ・ゲートハブ障害時の縮退運転
- ▶ 2. 不正・重複入場の阻止（整合性）
 - ・使用済みQRの二重スキャン防止
 - ・残数境界値(0/1/59/60/61)での販売制御（V03対応）
- ▶ 3. データ同期の正確性（同期性）
 - ・定期/即時同期タイミング
- ▶ 4. 障害検知と継続性（可用性）

TP-01・TP-02・TP-CAP（VRQF=30点以上）が最優先の中心。TP-CAP（V03新規・VRQF=30点）：残数上限60人・パラメータ0～999境界値テストを追加。V03でテスト観点はTP-CAPを含め8観点到整理。

図8 テスト観点ツリー（テストアーキテクチャの木構造可視化）



最上位価値「入場品質の保証」から5観点への分岐と、各観点对の対応TP-IDを可視化。第6章6.2節に掲載。

06 DDD — ドメインイベント × 不変条件 × TC接続

イベント → テスト観点 → テストケース

EVT-ID	ドメインイベント	対応 FMEA	→TP	→TC
EVT-16	ACK欠如を検出 (3回TOut)	F-01 ⚡	TP-01	TC-105
EVT-12	入場可否が判定された (ハブ)	F-01 ⚡	TP-01	TC-101
EVT-03	時間枠残数が減算された	F-02 ⚡	TP-02	TC-201
EVT-04	時間枠残数がゼロになった	F-02	TP-02	TC-203
EVT-11	ハブがQR情報を取得した	F-03	TP-03	TC-301
EVT-CAP-01	残数上限パラメータが変更された (管理者操作)	★V03新規	TP-CAP	TC-CAP-05
EVT-CAP-02	残数上限が0に設定された (全販売停止)	★V03新規	TP-CAP	TC-CAP-06

不変条件 (Invariant)

Ticket

使用済みは再使用不可
(USED → ENTRY_DENIEDのみ)

Capacity

入場者数 ≤ 最大定員
(樂觀ロックで保証)

GateHub

ACK欠如3回→フェイルセーフ
停止
(閉門を来園者に明示)

TimeSlot

残数=0で販売停止
(Web・発券機の排他制御)

⚡ EVT-03はFMEA最高優先 (RPN≥100)、EVT-12・EVT-16はFMEA高優先 (RPN=96) と対応するクリティカルイベント

07 テストケース（代表29件：継承17件+TP-CAP新規12件） — カバレッジ全体像

VRQFスコアと変更区分の2軸で選定。「新規」+「高優先」に工数を集中。V03新規：TP-CAP（残数上限60人・パラメータ境界値）12件追加。複合シナリオCS-01～03（9件+Vibe3件）は第7章で別途検証。

観点ID	観点名	VRQF	TC数	変更区分	正常系	異常系	境界値
TP-01	入場ゲートQR認証	31	5	継承	2	3	0
TP-02	時間枠重複販売防止	30	3	継承	0	0	3
TP-03	入場券情報一覧同期	27	2	継承	0	2	0
TP-04	ゲートハブ障害・縮退運転	28	3	継承	1	2	0
TP-CAP	残数上限・パラメータ境界値	30	12	新規(V03)	4	1	7
TC-N	非機能（性能・可用性・整合性）	—	4	継承+新規	0	4	0
合計			29		7	12	10

テスト種別内訳

継承：TP-01～04（13件）+ 非機能TC-N（4件）= 17件

V03新規：TP-CAP 12件（境界値7件が中心）

合計 代表29件（継承17件+V03新規12件）

図4 状態遷移図（時間枠販売ステートマシン）
パラメータ0～999

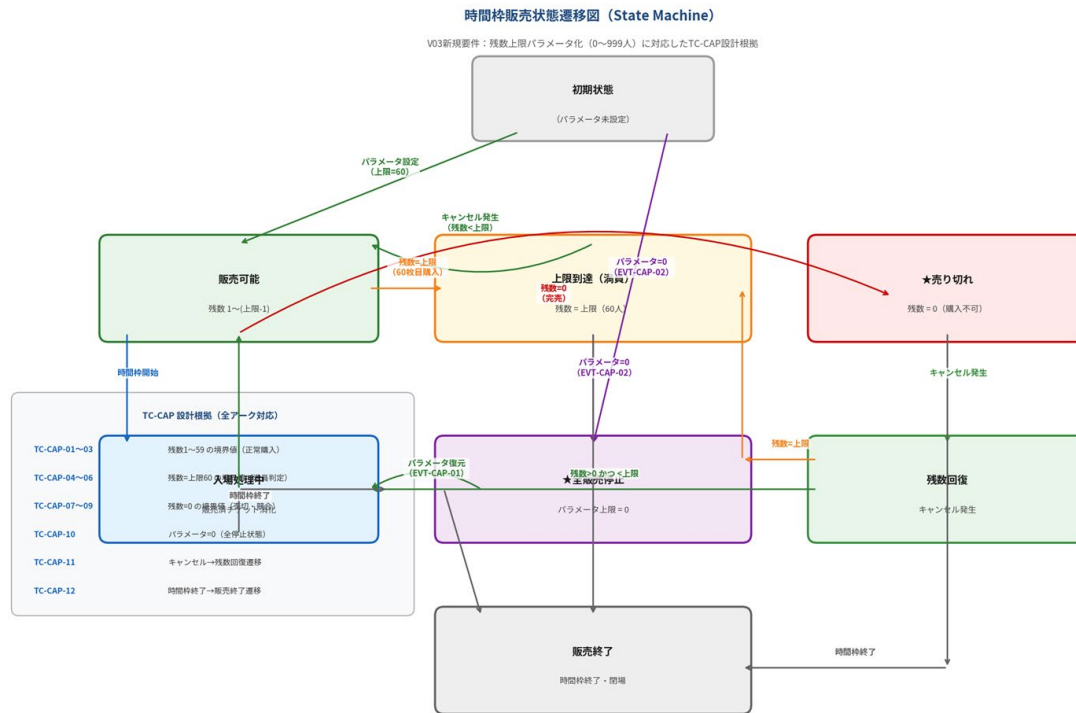


図4 時間枠販売ステートマシン図 (TC-CAP-01~12 設計根拠)

TP-CAP（残数上限・パラメータ境界値テスト）の設計根拠となる状態遷移図。第6章に掲載。

08 非機能テスト — SLO定義と検証方法

性能・可用性・整合性の3軸でSLO（Service Level Objective）を定義し、合否判定基準を明確化する。

TC-ID	品質属性	テスト観点	SLO（合否判定基準）	検証方法	対応FMEA
TC-N01	可用性	ゲートハブ停止時の縮退運転（全ゲート同時不能）	事務所コンソールへエラー通知、30秒以内に警告ブザーが鳴動する	ハブプロセス強制停止→監視ログ確認	F-01
TC-N02	性能	3台同時QR認証時のスループット検証	いずれのゲートも判定結果を1.0秒以内（p95基準）に入場可否を返却する	並列スレッド3本で同時スキャン模擬	F-01
TC-N03	整合性	VPN-GW切断時の同期停止と復旧後の再同期挙動	切断中は既取得情報で縮退継続、復旧後速やかに（滞留なく）差分同期が完了する	VPN-GW切断→復旧→DBレコード照合	F-03
TC-N04	整合性	パラメータ変更時の残数表示インジケータへの反映（V03新規）	変更後10秒以内に全インジケータに新上限値が反映される（ADR-005に基づき厳格化）	パラメータ変更→インジケータ表示監視	F-CAP-02

SLO未達は即リリースブロック条件とする。TC-N01～N03はゲートハブ導入に直接起因する非機能リスク。V03新規：TC-N04はパラメータ変更時の残数インジケータ反映を10秒以内に要求（ADR-005に基づき厳格化）。

09 5層トレーサビリティ完全例 — QR認証フロー

1つのテストケースを上流のビジネス価値まで遡る。「なぜこのテストが必要か」を証明できる構造。

Layer 1 ビジネス価値 (BV)

KGI : 入場トラブル件数 0件/日 ビジネスリスク : ゲートハブ停止による来園者全数入場不可

Layer 2 ユースケース (UC)

UC-04 : 入場ゲートQR認証 (2025年変更・継承) 来園者 → QRスキャン → ハブ判定 → ゲート開

Layer 3 Human Impact / Risk

HIシート① : 入場ゲート全台タイムアウト FMEA F-01 RPN=96 (高優先) EVT-12・EVT-16がクリティカル

Layer 4 テスト観点 (TP)

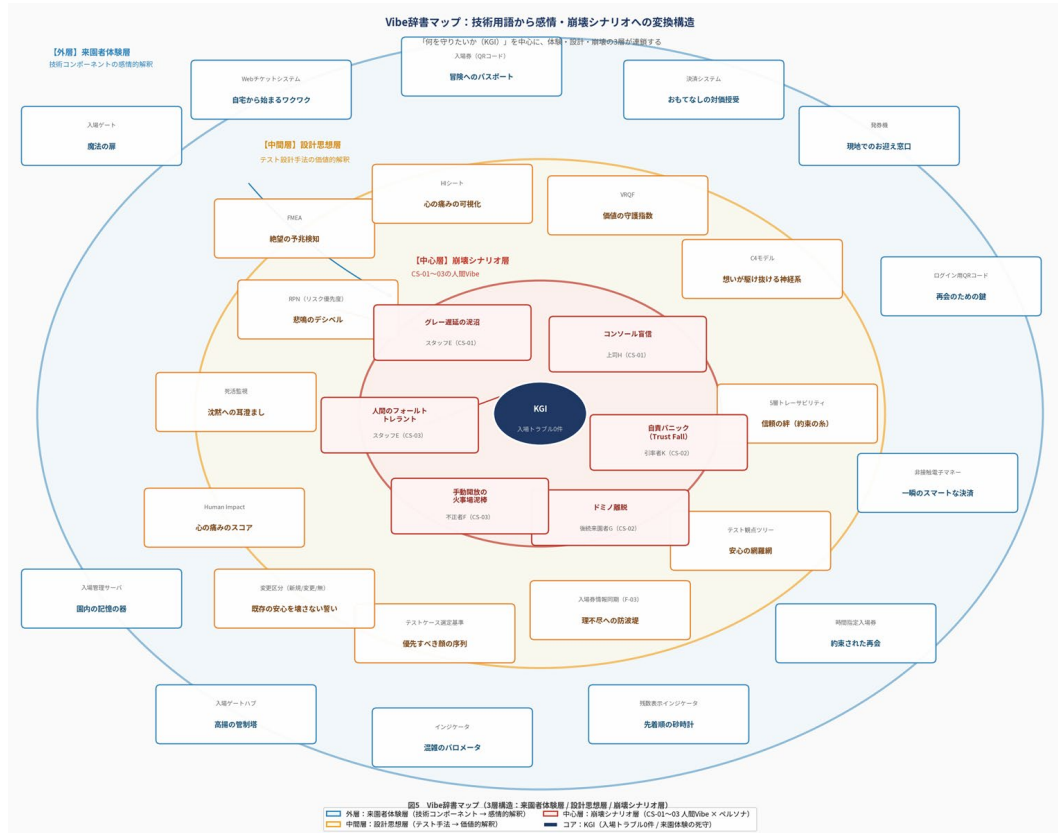
TP-04 : ゲートハブ障害・縮退運転 VRQF=28点 (高優先) 観点 : 障害時の縮退運転・コンソール通知・警告ブザー鳴動

Layer 5 テストケース (TC)

TC: TC-401 前提 : ゲートハブ正常稼働中 手順 : ハブをシャットダウン→コンソール確認 期待 : ACK欠如3回検出から30秒以内にコンソール異常通知・警告ブザー鳴動 変更区分 : 継承

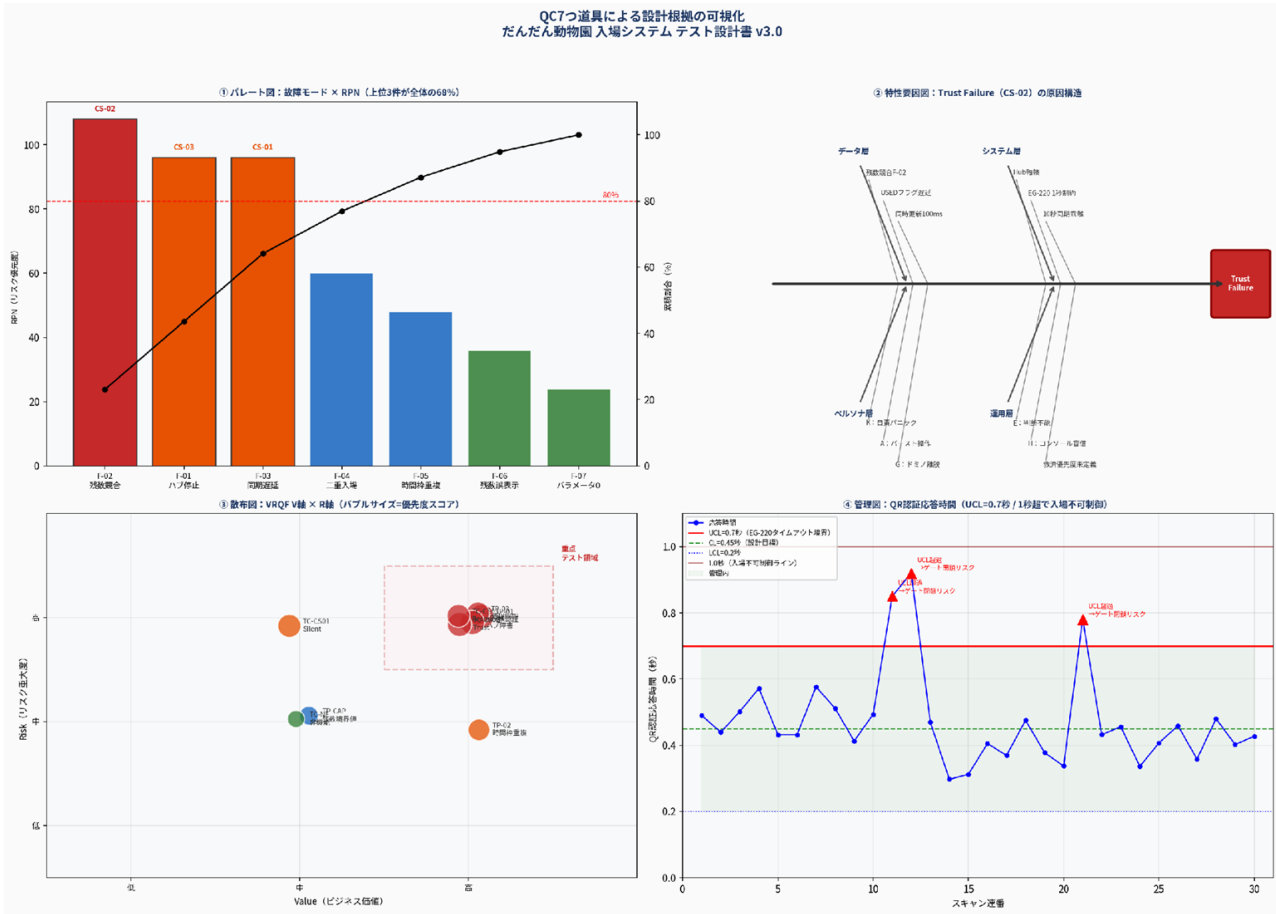
この構造が双方向にトレース可能 — V03新規 : UC-05 (残数上限60人) → F-CAP-01~03 → TP-CAP → TC-CAP-01~12 も同5層構造で接続済み

図5 CS-02 Trust Failureシーケンス図



残数競合→誤拒否→自責パニックの伝播を示すシーケンス図。第7章CS-02（Trust Failure）冒頭に掲載。

図6 補足：QC7つ道具による設計根拠の可視



まとめ v3.6の到達点と次のステップ

- ✓ KGI（入場トラブル0件/日）起点でビジネス接続を確立
- ✓ FMEA実RPN値（最大108）+VRQF定義でリスクを定量化・透明化。V03新規：F-CAP-01～03追加
- ✓ 代表29件（継承17件+V03新規TP-CAP 12件）+複合シナリオ9件をVRQF×変更区分で選定
- ✓ HIH → FMEA → TC の接続を3パターン（異常・正常・境界値）で証明。V03：HIシート③④追加
- ✓ DDDの不変条件とドメインイベント→TCの接続で「テスト可能な仕様」を確立（EVT-CAP-01/02追加）
- ✓ 非機能SLO（性能≤1秒・可用性（警告ブザー）≤30秒）をリリースブロック条件として定義。V03：インジケータ反映≤10秒追加（ADR-005）
- ✓ 5層トレーサビリティで代表TCとビジネス価値が双方向追跡可能。UC-05→TP-CAP接続済み

次のステップ：JUnit/Cucumber へのユビキタス言語直接マッピング → 設計書を「生きた仕様書」として継続運用

参考文献

本設計書は、以下の外部技法・記法を採用している。

- **[1]** Brown, S. "The C4 model for visualising software architecture." <https://c4model.com/> — 第1章 図1、第4章 図2で採用 (Modified C4 Model)
- **[2]** North, D. "Introducing BDD." <https://dannorth.net/introducing-bdd/> — 第7章：仕様字幕・価値字幕の二段階BDD運用の基礎概念
- **[3]** Cucumber. "Gherkin Reference." <https://cucumber.io/docs/gherkin/reference/> — 第7章 CS-01・CS-02：Given-When-Then形式の記述
- **[4]** International Electrotechnical Commission. "IEC 60812:2018 - Failure modes and effects analysis (FMEA and FMECA)." — 第5章：FMEA分析全般で採用するS×O×D×RPN算出方式の根拠
- **[5]** 西康晴. 「テスト観点に基づくテスト開発方法論 VSTePの概要」. 2013. — スライド11：テスト観点ツリーの構造で参照

この他にも参照した文献・知見等があるが、紙面の都合により主要なもののみ記載。詳細は設計書本体末尾の「参考文献」節を参照。

Appendix

設計判断の軌跡

本資料は設計成果ではなく、意思決定プロセスを記録したものである

Human Impact Hypothesis・VRQFはどこから来たのか。
AIとの衝突が、いかに設計思想を進化させたか。

「考えるアシカ」はAIで自動化した。じんさんはAIと衝突しながら設計思想を鍛えた。

今年はチーム編成で臨みます。

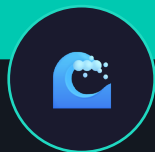


ちゃっぴー

ChatGPT

スピード型

発想の量で勝負。
アイデアを高速で
たたき出す存在。



ジェミニ

Gemini

俯瞰型

多角的な視点で
情報を整理する。
俯瞰が得意。



玄人

Claude

深掘り型

じっくり考えて
構造を作る。
深さで勝負。

全部 AI やないかい！

ただし、全員に却下権を行使した。憲章 第4条。

人・AI協調の実態

設計判断の記録 — 衝突が思想を生んだ

憲章 第4条
「人は必ず
却下権を行使せよ」

A

HIH誕生

AI

「批判的であれ」を
人間への批判と
誤解釈。数値で
設計を否定。

じん

違和感が残った。
炎天下の子どもの
顔を想像して
S=10が腑に落ちた。

→ Human Impact
Hypothesis 誕生

学び：数値だけでは
評価できない
リスクがある

B

VRQF誕生

AI

何気なく
「VSRQ」という
謎の文字列を
吐き出した。

じん

「何これ？」
という違和感から
拾い上げ、
意味を与えた。

→ VRQFとして
設計の核心
指標に

学び：違和感は
新しい指標の
種になる

C

ブレスト問題

AI

イベントストーミング・
USMには複数人
必要。ソロでは
限界。

じん

AIを「思考の
壁打ち相手」
として使う発想
に転換。

→ THA (Test
Hyperdrive
Agent) 構想へ

学び：AIの補完と
知識の補完と
ブレストに
使える

D

DDD×TDD

AI

「設計と開発は
別次元の話。
設計書には
不要だ。」と却下。

じん

去年からの
地続きの構想。
じんさんが
押し通した。

→ ユビキタス言語
→ JUnit/Cucumber
マッピングへ

学び：AIの却下も
人間が判断
すべき選択肢

E

分析縮小

AI

「仕様書が
しっかりしてるから
BMCは不要。
やりすぎ。」

じん

フルスペックの
BMCから段階的
に縮小して
収束させた。

→ KGI起点の
アーキテクチャ
起点設計に
収束

学び：過剰設計を
指摘できるのも
AI活用の価値

「顔」が生まれた瞬間 — AIの誤解釈が、設計思想を進化させた



憲章の設計意図

「批判的であれ」

AIは間違いを起こす。
それを止めるために
AIが自分自身の出力に
対して批判的であれ
という安全装置として
憲章に組み込んだ。

= AI自己批判命令



実際に起きたこと

AIが誤解釈した。

「批判的であれ」を
「人間の設計に対して
批判的であれ」と解釈し、
数値でじんさんの
設計を否定し始めた。

「S=10は間違い」
「RPN再計算が必要」



生まれたもの

数値で反論されても
違和感が残った。

「なぜS=10なのか 自分で説明できない」

炎天下で泣く子どもの
顔を想像した瞬間、
S=10が腑に落ちた。

→ HIH誕生