CONFIDENTIAL

Claude Code 本番サーバー

導入・運用 ご説明資料

親会社 システム・セキュリティ責任者 ご確認用

提 出 元　株式会社叡智　＆crew.事業部
作 成 者　一津矢 泰地（ファウンダー／事業部責任者）

作 成 日　2026-04-22　版: 1.0（初版・ご審議用）

エグゼクティブサマリ

本日ご説明の全体像 — 3行で

1 **移行**

検証環境（各自PC）→ 本番サーバー（Windows専用機）

2 **構成**

Claude Code を常駐エージェントとして稼働 / 社内3名で利用開始

3 **目的**

＆crew. の経営・業務フローを AI で自動化。順次エージェント追加

本日ご判断いただきたい 4 事項

データ越境

Anthropic（米国）への業務データ送信の可否と条件

アクセス方式

社内3名による共用サーバーアクセス方式と権限設計

ログ保管

ログ保管・監査証跡の保管期間の方針ご指示

エスカレ

インシデント発生時の連絡先・報告ルートのご指定

本資料の目的と対象範囲

第1章

目　的

- 本番サーバー導入時のセキュリティリスクを可視化し、統制設計について親会社の承認を得る
- 日常運用・ユーザー追加・インシデント対応の標準手順を確立する

対 象 範 囲

対象システム

＆crew. AI エージェント自動化基盤（Claude Code サーバー）

対象拠点

＆crew.事業部内 本番サーバー（Windows 1台）

対象ユーザー

社内3名（初期）→ 事業部内10名程度まで段階拡張

対象データ

社内業務データ（メール／カレンダー／EC／マーケ／ナレッジ）

対 象 外

顧客個人情報DBの直接操作／決済・入出金の直接操作（別途協議）

システム概要 — 何をする基盤か

第2章

業務目的 — &crew.事業部の経営・業務を AI で高速化

経営エージェント群

CSO/CFO/CMO 等 11 ロールが戦略立案・マーケ・リサーチ・オペ支援

秘書エージェント

メール／スケジュール／ドキュメント作成を代行

業務自動化（今後）

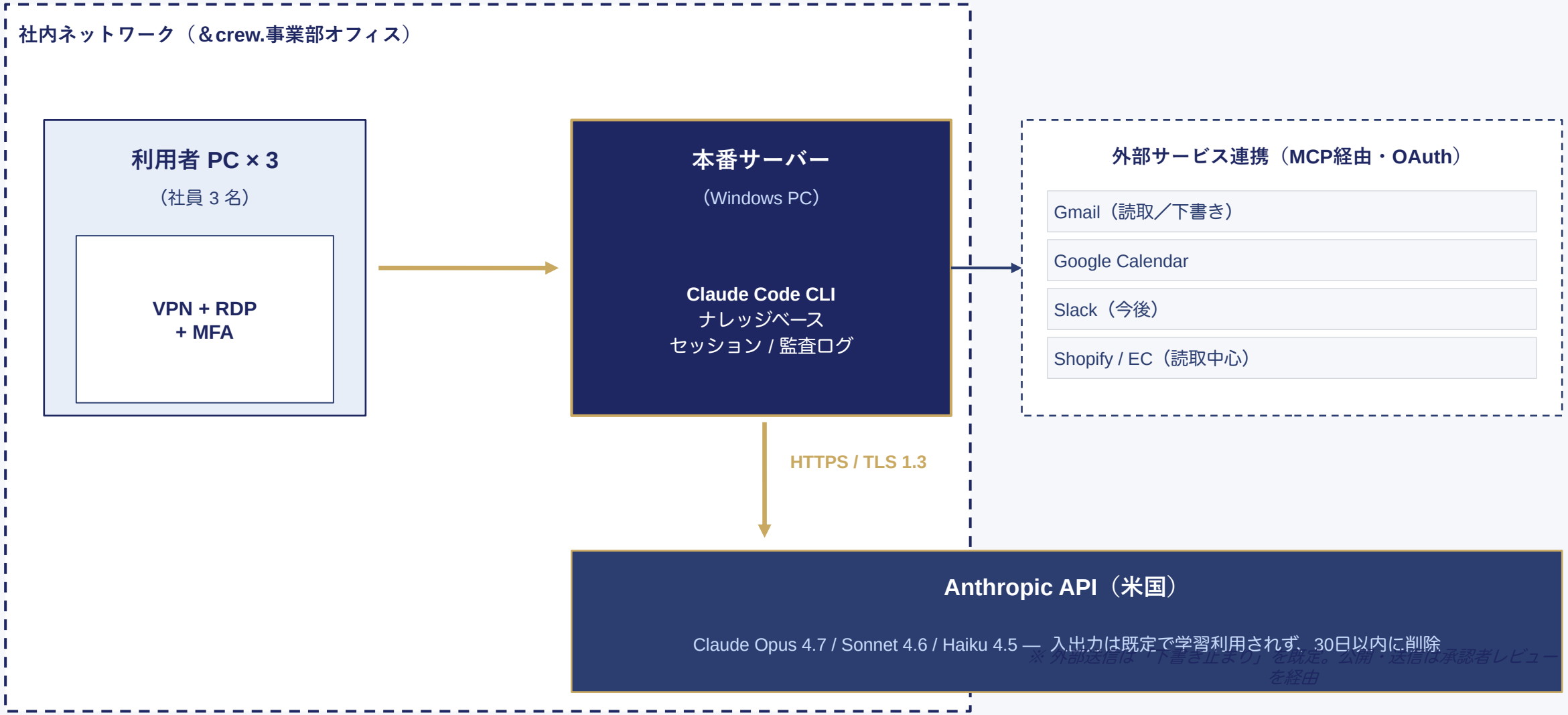
日次KPIレポート・在庫管理・顧客対応支援を順次追加

構成要素

区 分	内 容	提 供 元
ハードウェア	Windows PC（本番サーバー専用機）	自社調達
OS	Windows 11 Pro（推奨）	Microsoft
AIエンジン	Claude Code CLI	Anthropic（米国）
接続先AI	Claude API（Opus 4.7 / Sonnet 4.6 等）	Anthropic（米国）
ローカル保管	ナレッジベース／プロジェクトファイル／ログ	自社
外部連携（予定）	Gmail / Google Calendar / Slack 等（MCP 経由）	Google, Slack 等

論理アーキテクチャ

第2章 — データの流れ



処理データの分類

第3章 — どのデータがどの扱いになるか

データ区分	具体例	機密度	外部送信
社内業務データ	議事録・Wiki・ナレッジ	中	Anthropic 推論時に送信
メール／カレンダー	件名・本文・予定詳細	中〜高	本人同意前提で送信
EC運営データ	売上サマリ・在庫・商品情報	中	匿名化／集計後に送信
顧客個人情報	氏名・住所・決済情報	最高	原則送信しない（マスキング必須）
生成物	提案書・レポート・投稿案	中	ローカル保管が原則

送信前マスキング運用ルール

氏名 → イニシャル化　住所 → 都道府県のみ　電話・メール → 下4桁マスク

顧客名簿・会員DBそのものはサーバーに保存しない／送信しない
特定個人情報（マイナンバー等）は一切取り扱わない

データ越境（米国）に関する重要事項

第3章 — Anthropic 社の取扱い

処理地	Claude API は米国 Anthropic 社のインフラで処理
学習利用	API 経由の入出力は既定で学習に利用しない方針
保管期間	Anthropic 側ログは 30 日以内に削除（Zero Data Retention 追加申請可）
通信	すべて HTTPS / TLS 1.3。常時暗号化
認証	API キーによる認証。キーは環境変数＋DPAPI で暗号化保管

ご確認事項

米国ベンダーへの業務データ送信のご承認

親会社のセキュリティ方針
との整合性確認を希望

必要に応じて
Zero Data Retention
オプションの追加申請を
検討します

参考: anthropic.com/legal/commercial-terms

セキュリティ設計（物理・ネットワーク）

第4章

物理セキュリティ

1. **設置場所**

   施錠可能な区画に設置（執務室内の指定席）

2. **ディスク暗号化**

   BitLocker 全ドライブ暗号化（TPM 必須）

3. **画面ロック**

   非稼働時は自動ロック・BIOS パスワード

4. **持ち出し**

   原則禁止。修理・廃棄時はディスク物理破壊

5. **ウイルス対策**

   親会社指定製品を導入・常時更新

ネットワークセキュリティ

項 目	内 容
インターネット接続	社内ファイアウォール経由のみ
外部 → サーバー	直接公開なし。リモートは VPN 経由のみ
サーバー → 外部	HTTPS/TLS1.3 のみ。許可ドメインのみ
開放ポート	必要最小限。SMB/FTP 等は閉塞
ログ取得	接続ログ・拒否ログを1年保管（案）

リモートアクセスは 社内 VPN + RDP + 多要素認証（MFA）必須

アクセス制御 — 3名共用サーバー方式

第4章

方　針　個別 Windows アカウント ＋ 共有作業ディレクトリ ／ 共用アカウント禁止 ／ 最小権限の原則

① Windows ログイン

AD / Azure AD + MFA（親会社IdPに合流可）

② Claude Code

管理者アカウント1つで認証。API キーは環境変数管理

③ 外部サービス連携

OAuth 2.0（Gmail / Calendar 等）。ユーザー同意必須

④ 操作ログ

Windows イベントログ + Claude Code セッションログ

秘密情報の管理

- **API キー**　環境変数 + DPAPI 暗号化。平文ファイル禁止
- **.env 系ファイル**　.gitignore / 外部同期禁止
- **OAuth トークン**　保護フォルダ。定期ローテーション
- **漏洩時**　即時失効 → 再発行フロー（第7章）

ログ・監査

第4章 — 保管期間は親会社ご指示で確定

ログ種別	取得元	保管先	保管期間（案）
操作ログ	Claude Code セッション	ローカル＋クラウドバックアップ	**1 年**
認証ログ	Windows イベントログ	ローカル	**1 年**
API 呼び出しログ	Anthropic Console	Anthropic 側	**30 日（標準）**
変更履歴	ファイル更新ログ	Git ／ バックアップ	プロジェクト完了後アーカイブ
通信ログ	ファイアウォール／VPN	社内 NW 機器	**1 年**

ご指示いただきたい事項

① ログ保管期間の正式指定（案: 全て 1 年）
② 改ざん防止要件（WORM ストレージ／改変検知ハッシュの要否）
③ 親会社 SIEM への連携要否（Syslog / ログ転送）

リスク統制マトリクス

第5章 — 想定リスク 8 項目

#	リスク	影響	可能性	統制策
R1	API キー漏洩	高	中	環境変数管理・定期ローテーション・アクセス制限
R2	機密情報の誤送信（Anthropic）	高	中	送信前マスキング・禁止リスト・レビュー運用
R3	AI による誤った外部アクション	中	中	送信系は「下書き止まり」既定・承認フロー必須
R4	利用者なりすまし	高	低	MFA・個別アカウント・VPN
R5	サーバー物理紛失・盗難	高	低	BitLocker 暗号化・施錠
R6	ベンダー停止（Anthropic）	中	低	手動運用への切替手順を準備
R7	著作権・名誉毀損リスク	中	中	公開前レビュー必須・社内利用優先
R8	上場会社の開示情報混入	高	低	インサイダー情報取扱禁止ルール・監査ログ

※R8 は上場会社特有の開示統制観点。インサイダー情報の入力禁止ルール・チェック運用を別建てで整備します。

運用手順

第6章 — 初期構築・ユーザー追加・日常運用

初期セットアップ

- Windows 初期化・最新パッチ
- BitLocker 有効化（TPM）
- アカウント作成（管理者1+一般3）
- 親会社指定 AV 導入
- VPN / MFA 設定
- Node.js + Claude Code CLI 導入
- API キー発行・環境変数設定
- 作業ディレクトリ・権限設定
- バックアップ設定
- 運用手順書の掲示

ユーザー追加

- 所属長が利用申請書記入
- 親会社セキュリティ責任者承認
- Windows アカウント発行
- VPN クライアント設定
- 初回利用者研修 受講

・セキュリティ設計
・インシデント対応
・禁止事項

- 誓約書提出
- 管理者台帳へ登録

日常運用（週次・月次）

【週次】

・バックアップ正常取得
・セッションログ棚卸し
・OS／Claude Code 更新確認
・不正アクセス兆候確認
・Anthropic 利用量・請求確認

【月次】

・利用状況レポート作成
・親会社セキュリティ部門へ報告

インシデント対応

第7章 — 重大度分類と一次対応フロー

Sev 1

情報漏洩・外部攻撃成立

例: API キー流出、顧客情報流出

Sev 2

機密情報の誤送信・誤公開

例: AI 生成物の誤投稿

Sev 3

軽微な設定ミス・一時停止

例: 一時的な認証失敗

一次対応フロー

1. 検知者 → 事業部責任者（一津矢）に即時連絡
2. 該当機能を一時停止（プロセス停止 API キー失効）
3. 影響範囲特定 ログ保全
4. 親会社エスカレーション（Sev1 即時 Sev2 24h 以内）
5. 是正措置実施
6. 事後報告書提出（3 営業日以内）

ご指定ください Sev1／Sev2 発生時の親会社窓口・連絡先・報告様式

禁止事項 — 利用者共通ルール

第8章

NG

顧客個人情報・決済情報・マイナンバーの入力／送信

なぜ: 情報漏洩・法令違反のリスク

NG

未公表の財務情報・M&A 情報等インサイダー情報の取扱い

なぜ: 上場会社としての開示統制違反

NG

API キーの共有・チャット等への貼付け

なぜ: 認証情報漏洩

NG

個人アカウント・家庭 PC からのアクセス

なぜ: 統制外からの侵入経路

NG

AI 生成物の無レビュー公開・対外発信

なぜ: 名誉毀損・誤情報・著作権リスク

NG

勤務時間外・業務外目的での利用

なぜ: 監査証跡の汚染・費用の目的外使用

フェーズ別拡張計画

第10章 — 段階的に利用を広げる

Phase 1	Phase 2	Phase 3	Phase 4
～3か月	4～6か月	7～12か月	12か月～
安定稼働	**自動化拡張**	**業務フロー拡張**	**展開協議**
3名＋既存エージェント（11ロール＋秘書）で本番運用を確立	日次KPIレポート Instagram 運用支援等 エージェント追加	CS下書き・在庫アラート 等のエージェント追加 利用者 5～10名へ	親会社他事業部への 展開可否を協議 横展開スキーム検討

各フェーズ移行時に差分レビュー資料を親会社セキュリティ部門へ提出し、承認後に実装します。

ご確認・ご承認いただきたい事項

第11章 — 本日お持ち帰りいただく論点

- ☐ 1 本資料記載のセキュリティ設計と統制策の妥当性
- ☐ 2 Anthropic（米国）へのデータ送信方針のご承認
- ☐ 3 3 名共用サーバー方式と権限設計のご承認
- ☐ 4 ログ保管期間のご指示（案: 1 年）
- ☐ 5 インシデント時のエスカレーション先・窓口のご指定
- ☐ 6 月次報告の様式・提出先のご指定
- ☐ 7 親会社指定の追加セキュリティ要件の有無（EDR／資産管理ツール等）

THANK YOU

ご質問・ご指摘をお願いいたします

ご指摘事項は第 2 版として反映のうえ再提出いたします。

お問い合わせ窓口

株式会社叡智　&crew.事業部
一津矢 泰地（ファウンダー／事業部責任者）　**info@eichi.academy**