

# 株式会社ニッコー

---

DX戦略



## 1：企業経営の方向性及び情報処理技術の活用の方向性

持続可能な企業体制の確立とDXを活用した業務革新による次世代型ビジネスモデルへの転換

当社は、持続可能な企業体制の確立と次世代型ビジネスモデルへの転換に向けて、「データ活用×自動化×標準化×組織力強化」を軸とした取り組みを推進しています。

クラウドやAI・IoTなどの先進技術を活用した業務の効率化と自動化、蓄積データを活かした戦略的意思決定や保守サービスの高度化、標準機比率の向上による事業の安定化、そしてDX人材の育成と組織体制の強化により、変化に強い次世代型の経営基盤の構築を目指しています。

株式会社ニッコー  
代表取締役 佐藤 一雄

## 2：企業経営及び情報処理技術の活用の具体的な方策

当社は、経営ビジョンの実現に向け、「データ活用」を軸とした業務変革を推進しています。

営業活動においては、SFA（営業支援システム）を通じて取得した商談履歴・顧客属性・案件進捗などの営業データを分析し、見込み顧客の選定精度を高め、最適なタイミングでの提案を実現しています。

また、製品に搭載したセンサーから収集される稼働状況・異常ログ・稼働時間などの機器データをIoTプラットフォーム上で可視化・解析し、部品の劣化予測や故障前のメンテナンス提案を行う予防保全型の保守サービスを提供する準備を行っています。

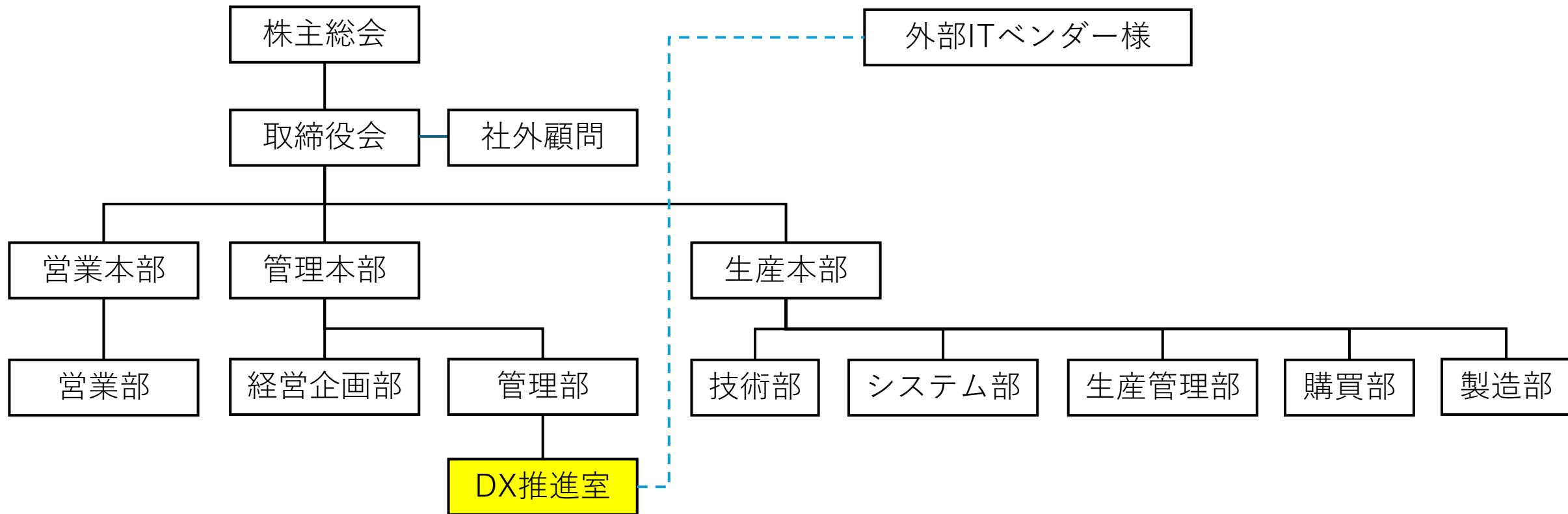
さらに、社内業務においては、申請書類・作業日報・在庫管理などの紙ベースの情報を電子化し、ワークフロー自動化ツールと連携することで、承認業務の迅速化や入力ミスの削減を図っています。

これらの取り組みにより、属人的な判断や業務処理から脱却し、蓄積データに基づいた全社的な意思決定とサービス提供が可能なデータドリブンな業務体制を構築しています。

あわせて、DX人材の育成にも注力しており、DX関連資格の取得を推奨するとともに、社内外の研修やセミナーへの積極的な参加を促進し、社員のスキル向上と意識改革を図っています。

## 2 - ①：戦略を効果的に進めるための体制

当社ではDX方針に沿った戦略を実施する為、専門のDX推進室を組織しております。  
また、弊社社外顧問や外部ITベンダー様とDX推進における協力体制を整えております。



## 2 – ②：最新の情報処理技術を活用するための環境整備

---

当社では、DX戦略の実行に向けて、最新のITシステム環境の整備を段階的に進めています。

営業領域では、SFA（営業支援システム）を導入し営業活動データをリアルタイムに収集・分析できる仕組みを構築しました。

IoTプラットフォームでは、各機器から稼働データを自動収集し、異常検知や保全提案につなげる基盤を整備しています。

社内業務のデジタル化においては、従来の紙・Excelベースの業務プロセスから脱却し、MS365を活用したワークフロー自動化を推進。レガシーシステムとの共存を前提に、順次刷新やデータ移行も計画的に進行中です。

### 3：戦略の達成状況に係る指標

---

- **営業領域におけるデータ活用の定着度**

- SFA活用率 (SFAに入力された案件数／全案件数)
- リードタイム短縮 (初回接触から受注までの平均日数)

- **IoT保守サービスに関する効果測定**

- IoT経由で取得された機器データ項目数の推移

- **社内業務の効率化に関する指標**

- 業務プロセスの電子化率 (紙→電子への移行状況)
- ワークフロー導入による決済時間の削減率

- **DX人材育成の取組状況**

- DX関連資格の取得者数
- 研修・セミナー参加人数

## 4：効果的な戦略の推進等を図るために必要な情報発信

---

本項目に関する当社の取り組みにつきましては、本資料の該当箇所にて詳細を記載しております。

当該資料は、弊社ウェブサイトにて一般に公開しており、どなたでもダウンロードいただけます。

## 5：情報処理システムにおける課題の把握

---

当社におきましては、これまでに独立行政法人情報処理推進機構（IPA）が提供する「DX推進指標 自己診断フォーマット」を用いて現状の自己評価を実施致しました。

その結果、抽出・認識された課題につきましては、本資料に示すDX戦略に基づき、現在、具体的な対応策の検討および実行を鋭意進めております。

## 6：サイバーセキュリティに関する対策

当社では、DX戦略の推進にあたり、サイバーセキュリティ経営ガイドライン（経済産業省・IPA）に基づき、以下の方策を講じています。

また、PCの資産情報と操作ログをリアルタイム収集し必要に応じて管理者が確認してます。

- **情報資産の保護とアクセス管理**

営業データやIoT機器データなどの重要情報に対し、アクセス権限の適正化やログ管理を実施。

- **クラウドサービス利用時のセキュリティ確保**

SFAやIoTなどのクラウドサービスにおいて、通信の暗号化や多要素認証を導入し、安全な利用環境を構築。

- **人的リスクへの対応**

情報漏洩対策として、全従業員にセキュリティ研修を実施し、リスク意識を醸成。

- **インシデント対応体制の整備**

不正アクセス等への備えとして、社内ルールと対応手順を整備し、迅速な対応が可能な体制を構築。