kintone Enterprise Circle

kintoneガバナンスガイドライン

2022年6月

サイボウズ株式会社

kintone

目次

【 1 】

はじめに

1.1.本ガイドラインの作成背景と目的

- kintoneはマウス操作で簡単にアプリを作成できるノーコード/ローコード開発ツールで「現場が主体となってアプリを作成できる」という特徴があります。その特性を生かし、業務で必要なシステムを業務担当者自身で開発していくことができます。

- 一方で**kintoneを利用する部門や対象業務が多岐にわたる**場合は、**アプリの品質確保やリスク管理のためにどうガバナンスを構築するか**は避けて通れないテーマとなります。

- kintone大企業向けユーザー会「kintone Enterprise Circle(kintone EPC)」においても、ガバナンスについて度々議論を交わしてきました。そのなかで、kintoneを利用している企業がそれぞれ**自社状況に応じて自分たちのガバナンスを構築できるよう**、この度本ガイドラインを作成し公開することになりました。

- 本ガイドラインを参照いただくことで、自社に合ったガバナンスを構築したうえで、kintoneを安心、安全に利用し、持続可能な形で業務改善を行っていただけると幸いです。

1.2.kintoneの特性と考慮すべきポイント

kintoneの特性

- 一般的に、ビジネス向けのノーコード/ローコード開発ツールは、高度なプログラミング知識などを必要としない、という特徴があります。
- そのなかでも、kintoneは特に業務部門での導入割合が高く、エコシステムの多彩やユーザーコミュニティの活発さから、現場担当者が自ら、様々な業務で利用できるシステムの開発を進めていく特性があります。

ガバナンス検討時の考慮すべきポイント

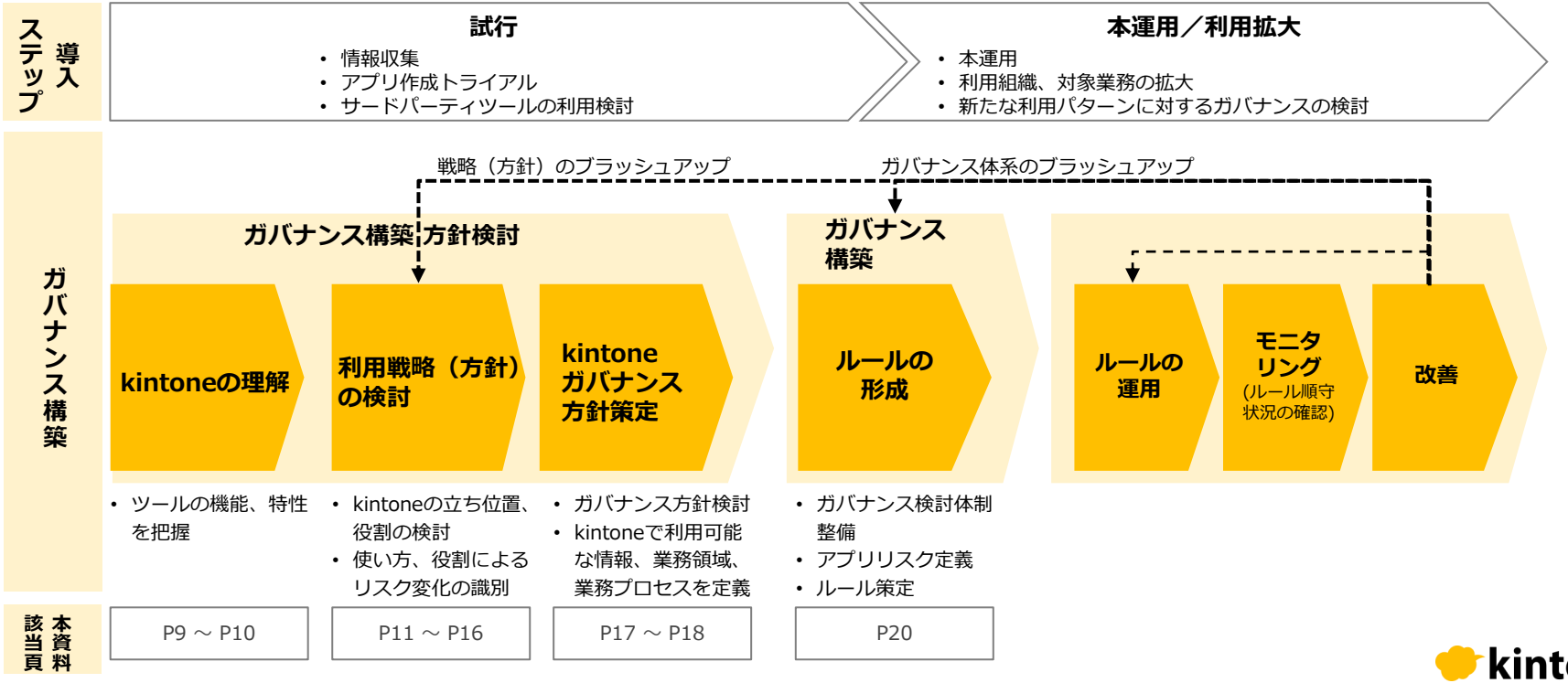
- kintoneの利用領域や利用者の拡大とともにリスクに応じたガバナンスの構築が必要となってきますが、業務部門が現場で自らシステム開発できることでのスピード感や柔軟性など、**kintoneが持つ特性とのバランスを考慮**し検討を進めることがkintoneを安全、安心に活用するポイントとなります。
- そのため、画一的にガバナンスを適用するのではなく、自社の利用状況や方針などの特性に応じ、**「何を守らなければならないのか」**、**「kintone利用においてどのようなリスクが生じるのか」**について十分に検討しガバナンス構築を進めることが必要になります。

【２】

kintoneガバナンス方針策定のポイント

2.1.ガバナンス構築手順(1/2)

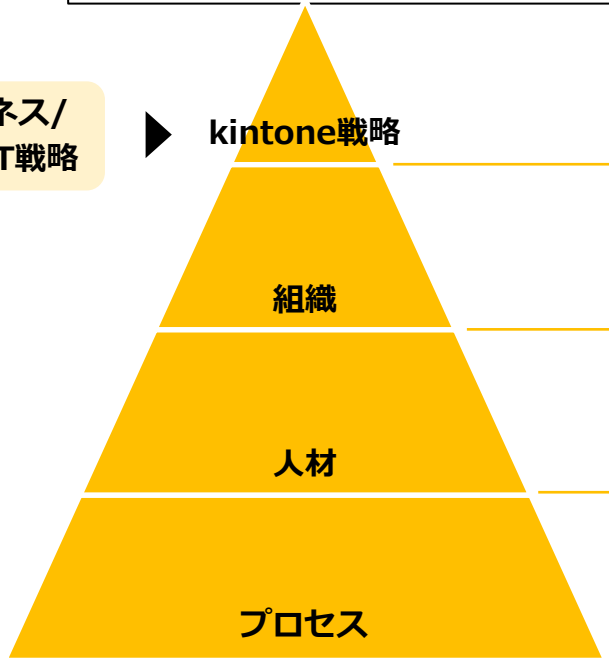
- kintoneガバナンス構築では「**kintoneの役割、利用戦略、利用パターンに伴うリスク**」を想定した検討が必要です。
- 下図では、導入ステップに合わせたガバナンス構築の検討ポイントと、検討ポイントの内容を説明している該当頁を表しています。



2.1.ガバナンス構築手順(2/2)

- ガバナンスを検討するうえで**「戦略」「組織」「人材」「プロセス」のそれぞれの領域を組み合わせて検討する**ことが重要であり、特定の領域に偏っていたり、欠けていたりする場合、ガバナンスの効果を十分に得られないことも考えられます。
- それぞれに求められる要素は利用企業によって異なりますので、以降の「利用戦略（方針）の検討」および「kintoneガバナンス方針策定」ステップにおいて、これらの領域を意識しながら検討を進めていくことがポイントになります。

ビジネス/全体IT戦略



- kintoneに対する理解
- kintone導入目的/活用方針
- kintoneアプリにおけるリスク認識

- kintone推進における役割・責任
- kintone導入における管理体制
- kintone業務部門の役割・責任

- kintone導入目的・方針の浸透・定着化
- kintone導入にかかわるリスク認識、コンプライアンス意識の熟成
- 利用領域に応じたアプリ作成者の育成
- デジタル人材の育成

- kintoneアプリのリスク評価・管理プロセス
- kintoneアプリの作成・変更 / 運用プロセス
- kintoneアプリにかかわるデータへのアクセス
- 情報漏洩・各種法令・内部統制・コンプライアンス対応
- kintoneリスク管理状況や導入効果のモニタリングプロセス

2.2.kintoneの理解

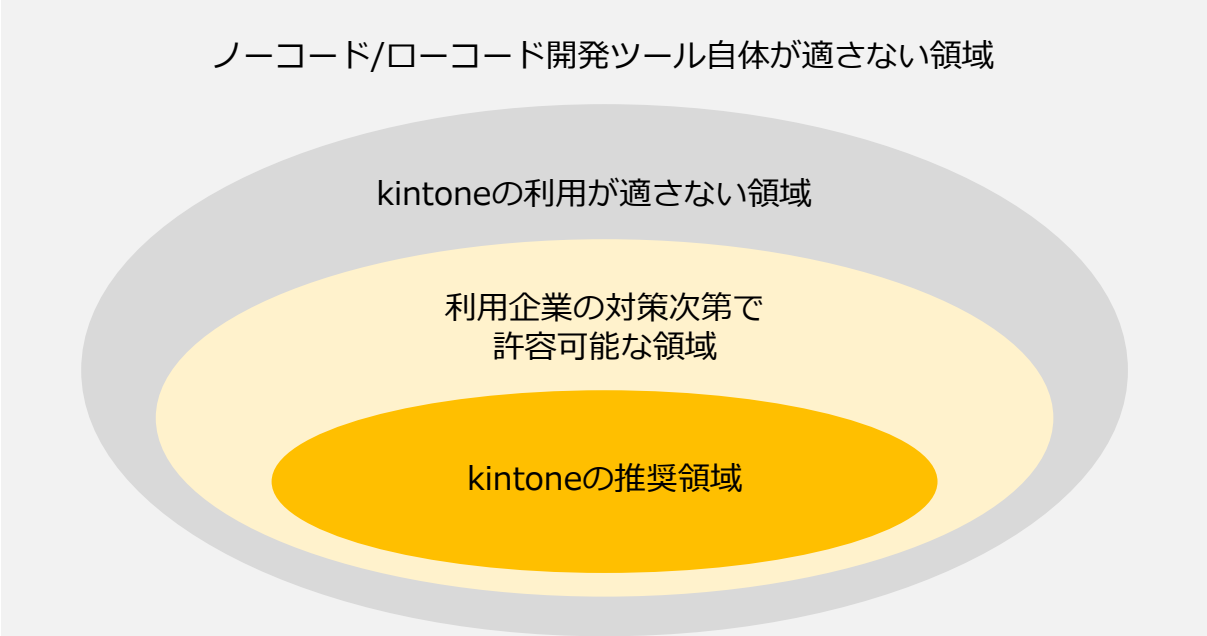
- 一般的に、ITツールの導入時には、**ツールの機能や特性を理解する**ことが重要です。ツールの特性を理解した上で、ガバナンス方針を検討することで、実運用に適したガバナンスを構築できます。
- kintoneにおいても、Webサイトやマニュアルなどから情報を収集したり、実際にkintoneを操作したりすることを通じて、kintoneの機能や特性を理解してください。

kintoneの理解イメージ

【参考】2.2.kintoneの理解

- 各種開発ツールには、いずれもツール毎の特性があり、利用する領域に向き／不向きがあります。
- kintoneについてもツールの特性を考慮して利用範囲を決定する必要があります。**利用企業の対策次第で適用できる範囲は変化します**。

業務領域へのkintone適用イメージ



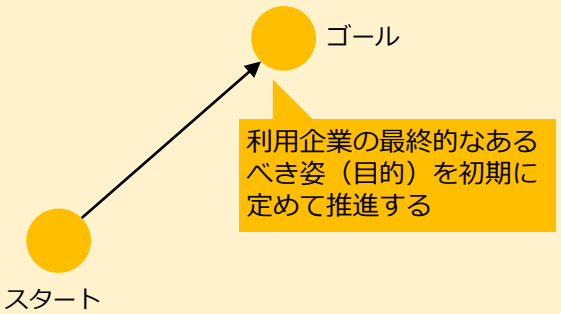
2.3.利用戦略（方針）の検討（1/5）

- kintoneの機能や特性を理解した後、kintoneの展開方式を検討します。一般的に、ツールの展開方式は「ターゲット固定方式」と「ムービングターゲット方式」の2種類あります。
- kintoneは効果測定しながら利用を広げていくのが有効なツールであるため、「ムービングターゲット方式」のように**適宜アップデートしていく**ことが重要になります。

kintone展開方式

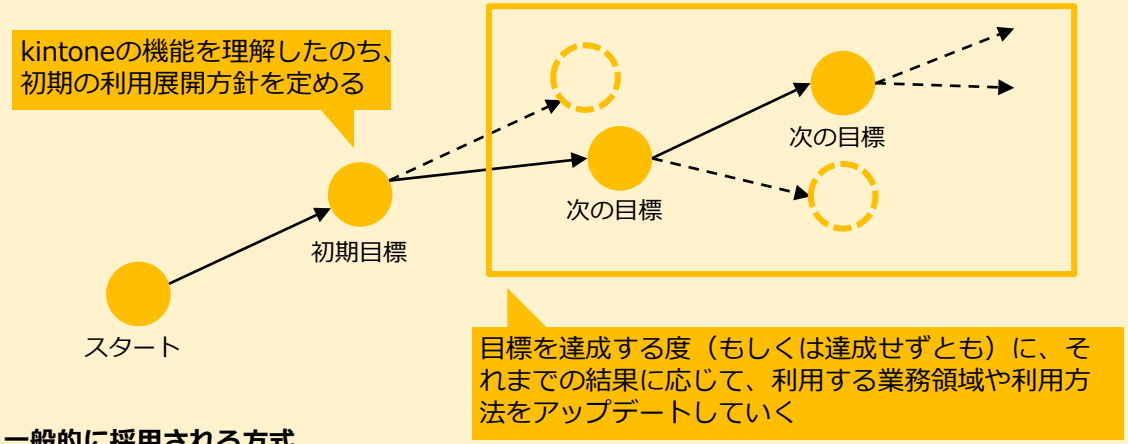
ターゲット固定方式

最終ゴールを定め、一気に展開する方式



ムービングターゲット方式

直近（1～2年）で達成する目標を定め、定期的に目標を見直す方式



※一般的に採用される方式

2.3.利用戦略（方針）の検討（2/5）

kintoneの利用戦略を考える上では、全社のIT戦略と照らし合わせながら、**kintoneの利用領域を定めること**、**kintoneの担い手となる人材について検討すること**が重要なポイントとなります。

kintone利用戦略の考え方のポイント

全体IT戦略

組織における**kintoneの利用適正領域**や現状の**kintone活用状況**を考慮

キーとなるkintone戦略要素の検討

〈利用領域〉

- 適用する業務領域
- 適用する業務プロセス
- 利用可能とするデータ
- 他ツールとの関連性

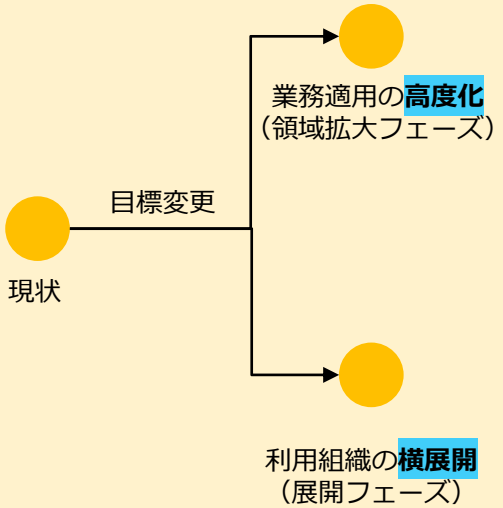
〈人材〉

- 全体IT戦略に合わせた人材像の検討
- kintone利用を許可する組織や人材を定義
- 戦略に合わせた人材育成方法

2.3.利用戦略（方針）の検討（3/5）

- kintoneの利用戦略は適宜見直すことが一般的です。
- 戦略の見直しは、**kintoneの適用領域を拡大する**とき、あるいは、**kintoneの利用を他組織へ横展開していく**ときに実施します。

kintone戦略の見直しの考え方



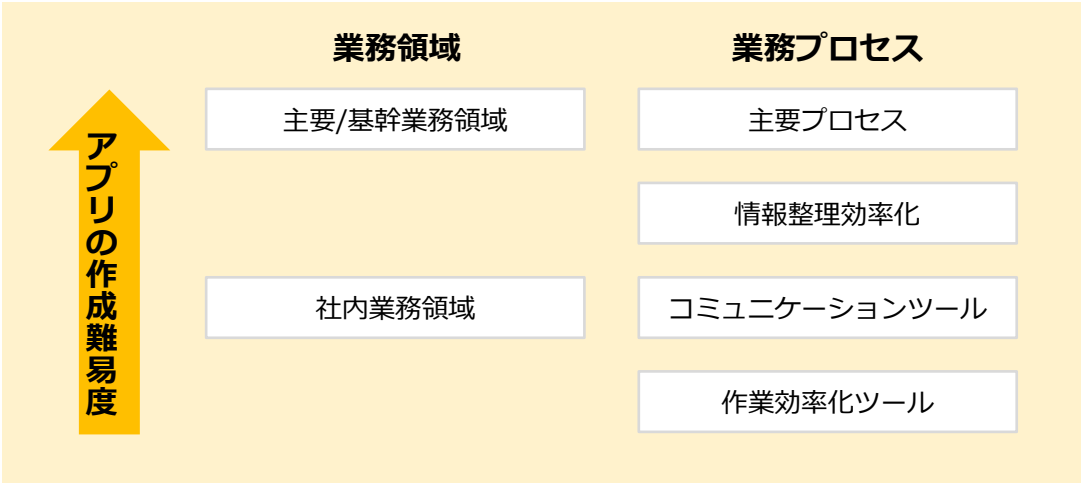
現状のkintoneの適用領域を深耕し、**より機密性や完全性、可用性が求められる領域のアプリ作成**を実施します。アプリの作成が高度化、複雑化するため、kintoneアプリ作成の熟練者が必要となります。

現状のkintoneの適用内容を**他組織へ横展開し、利用を拡大**します。横展開する際は、展開先の組織におけるkintoneアプリ作成環境の整備状況や、アプリ作成者のスキルレベルに合わせて拡大していくことが必要となります。

2.3.利用戦略（方針）の検討（4/5）

- kintoneの利用戦略を検討するにあたり、リスクの把握も大切です。**「業務領域」「業務プロセス」「利用データ」の観点で、どのようなリスクがあるか**を整理します。
- 以下はkintone利用領域におけるリスクの一例です。下図を参考に、自社のkintone利用状況に応じたリスクを確認してください。

利用領域の選定にて検討するリスクレベルの例



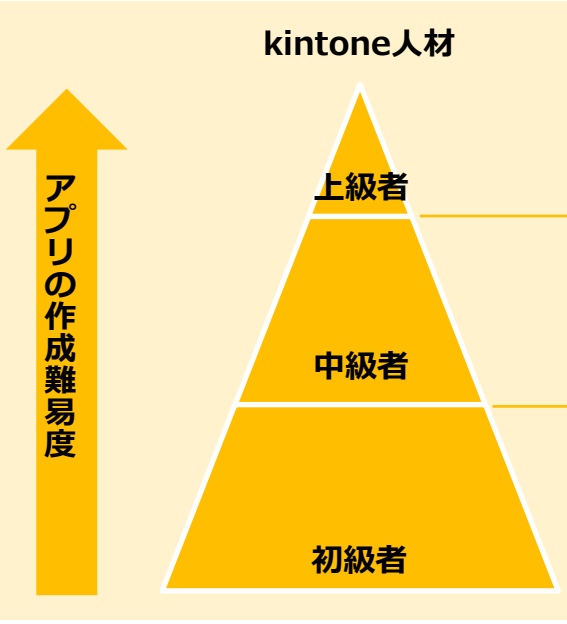
適用する業務領域や業務プロセスに応じて、求める可用性が異なるため、それを実現するためのアプリの作成難易度（パフォーマンスの確保を含む）に影響を与えます。

クラウドサービスにどこまで機密性の高い情報を保存するかは、全社ルール含めた対応が必要です。

2.3.利用戦略（方針）の検討（5/5）

- 人材の育成も重要な要素の一つです。
- **ある程度の機能理解を持ったkintone中級者がリスクを理解し、上級者へステップアップする**ことが、kintone人材の底上げやアプリの作成難易度に応じたアプリ作成者の配置につながります。

人材戦略・人材育成の考え方の例



上級者

kintoneの特性を熟知し、リスクに応じたアプリ作成を行える人材です。
アプリの可用性や完全性が求められる領域は、必然的に作成難易度が上がるため、上級者のみにアプリ作成を限定することも必要です。

中級者

一定程度kintoneの機能を理解し、幅広い活用が検討できる人材です。
一方で、機能を知っていることで、いつの間にか高リスク領域を扱ってしまう可能性もあり、経験値に合わせてリスクも勘案し上級者へ進むプランを策定するとともに、高リスク領域のアプリ作成を制限する仕組みも必要です。

初級者

kintoneで初めてシステム開発する、もしくはシステム開発の知識を持たない一般利用者にあたる人材です。作業改善等で積極的にkintoneを活用するため、広く利用を開放しますが、人数も多くなるため計画的な人員配置の検討が必要になります。また、高リスク領域のアプリ作成には踏み入れないような仕組みも必要です。

【参考】2.3.利用戦略（方針）の検討

kintoneの利用戦略が検討が進むと、それに合わせて必要となるガバナンス方針やルールが見えてきます。

kintone利用戦略とそれに伴うガバナンス方針やルールの例

事例１

【戦略】
コミュニケーションロス防止・効率化のためにkintoneを活用

【ガバナンス方針やルール】

- 有効な利用となるよう利用組織の横展開および利用者の拡大
- 機密性の高いデータを利用しないようルール作成

事例２

【戦略】
既存業務プロセスからデータ取得し、整理するためにkintoneを活用

【ガバナンス方針やルール】

- 対象業務を利用する人達のkintoneナレッジ向上
- 利用可能なAPIや3rd Partyの選択・整理
- 機密性の高いデータを利用しないようルール作成

事例３

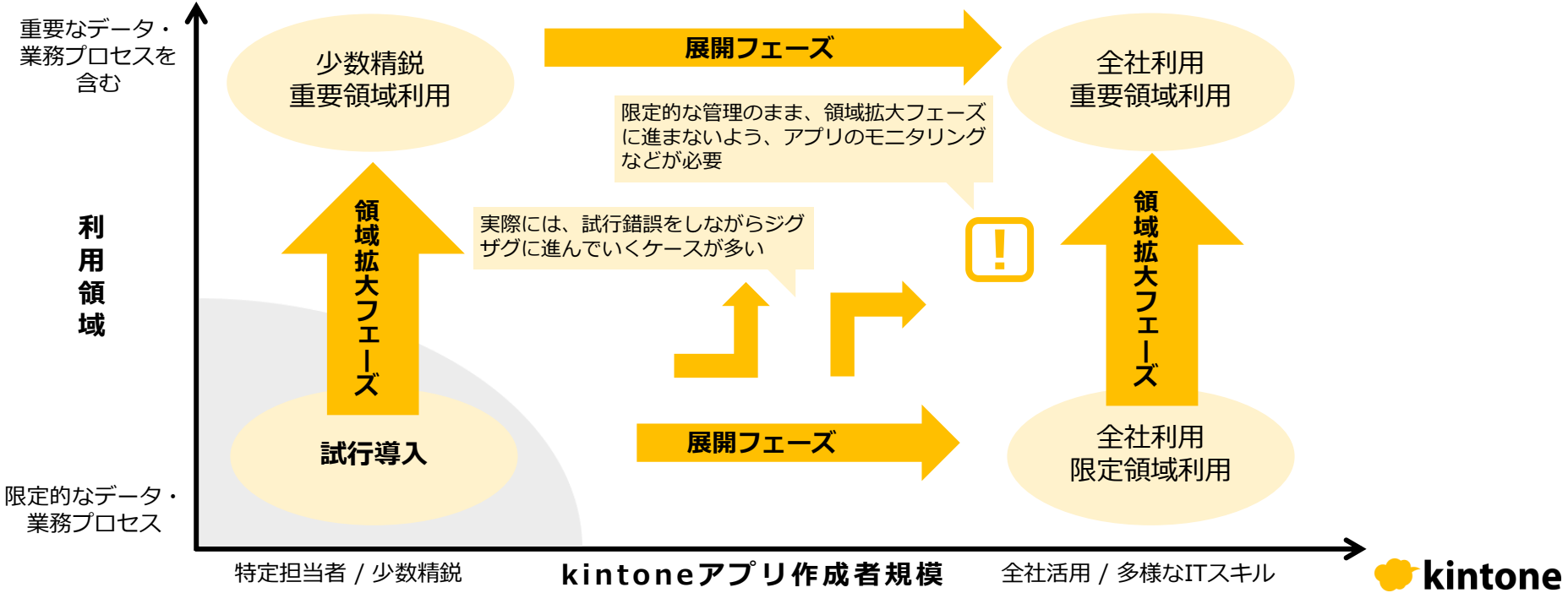
【戦略】
基幹システムをkintoneにて構築

【ガバナンス方針やルール】

- 不具合を発生させないために組織や人材を限定
- プロフェッショナル人材の育成
- 既存の開発プロセスと同等レベルのプロセス適用

2.4.ガバナンスマップ（1/2）

- 下図は、kintoneの「利用領域」と「kintoneアプリ作成者規模」の二軸で表現したガバナンスマップです。
- **自社がどのポジションにいるのかを把握するだけでなく、今後どのようなポジションに進みたいのかを検討する**ことで、ガバナンスのあるべき姿を理解できるため、ガバナンス体制やアプリの運用ルールなど、適切なガバナンス構築に繋がります。



2.4.ガバナンスマップ（2/2）

- kintoneの領域拡大フェーズと展開フェーズにおけるガバナンス検討ポイントを例示しています。
- ただし、自社の戦略やアプリの特性によって、考慮すべきリスクが異なるため、**kintoneの利用状況に応じて「組織」「人材」「プロセス」の最適なガバナンスを検討**してください。

フェーズ	考慮すべき主なポイント	ガバナンス検討ポイント
領域拡大フェーズ	**データ漏洩** リスクの高い情報を扱うことで、不適切なアクセス権の設定等に伴いデータの機密性が侵害されるおそれがある。 **不正確な処理** リスクの高いプロセスを扱うため、作成上のミスまたはアプリへの不適切なアクセス権の設定等に伴い、アプリの処理の完全性/可用性が侵害されるおそれがある。	• リスクに応じた作成権限、チェック体制 • アプリ作成/変更時の第三者確認、深度 • データガバナンスに関連する対策
展開フェーズ	**シャドーIT（野良アプリ）** アプリ作成者が多様化するため、作成されたアプリが無管理のまま放逐される、または、意図しないアプリが作成されるおそれがある。 **アプリ作成者のスキル不足による作成ミス** アプリ作成者が多様化し、ITスキルやkintoneへの理解が不足しているアプリ作成者が増えることで、処理ロジックが不正確なアプリが作成されるおそれがある。	• 全社的な管理体制 • 全社的な教育活動、段階的な教育制度設計と作成許可 • アプリ一覧管理、モニタリングの高度化

【３】

kintoneガバナンス構築のポイント

3.1.kintoneガバナンスの全体像

- kintoneにおけるガバナンスは、マネジメントによって承認された利用ルールを、推進組織が全体を通した実効性を担保しつつ、業務部門が定められたルールを遵守しながらアプリの作成や運用を行います。
- なお、各組織の在り方や役割については自社の状況に応じて検討が必要です。

kintone

3.2.個別アプリのリスク評価

- kintoneでは多種多様なアプリが作成可能であるため、アプリに対するリスク評価が重要となります。
- アプリごとのリスクは**使用されるデータ/関連する業務プロセスの重要度等をもとに各社ごとに検討することが必要**です。
  以下はアプリのリスク評価を行う際の一例になります。

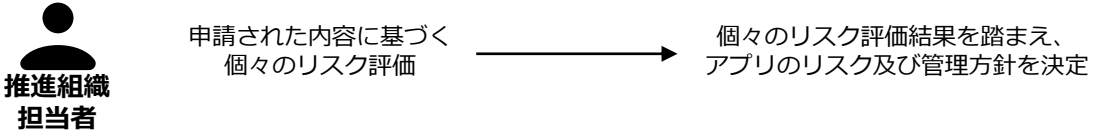
アプリ作成申請

申請フォームの例

【業務プロセス】
- 対象業務
- 顧客業務での利用があるか
- J-SOX上の評価対象システムとなるか

【データ】
- 格納する主要なデータ
- 格納を予定しているデータの数
- 格納するデータにおける個人情報の有無

アプリのリスク評価



リスクと判断基準の例

【kintoneに格納したデータが漏洩する】
- データの格納件数が1,000件以上であれば、リスク中、10,000件以上であれば、リスク高。
- 個人情報が格納される場合は、リスク高。

【kintoneアプリのエラーにより業務が停止する】
- 中核業務（生産等）に利用される場合は、リスク高。
- 内部業務のみの利用の場合は、その業務の重要度に応じて、リスク中またはリスク低。

アプリ管理方針の例

【リスク高が5つ以上】
kintone以外での構築を検討する。

【リスク高が2つ以上4つ以下】
高リスクのアプリとして厳格な管理体制の元で管理する。

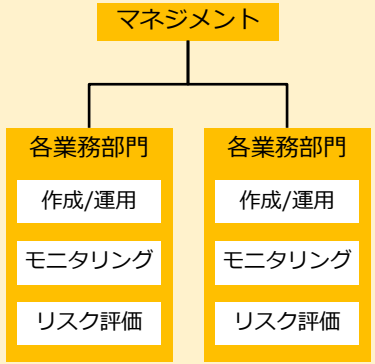
【リスク高が1つ以下】
一部管理を緩和した運用を容認する。

3.3.主な対応策(1/5) -組織・体制-

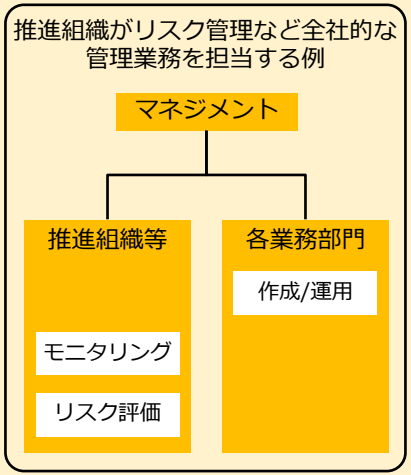
- kintoneの利用を推進しつつ、適切なガバナンスを構築、維持するためには組織・体制の検討が必要です。
- 自社の戦略（方針）に応じて、ガバナンスの管理業務を特定の組織に集約するのか、あるいは、複数の部門に分散するのか、組織の規模をどうするか、**kintoneの利用状況や成熟度に応じた段階的な検討が必要**になります。

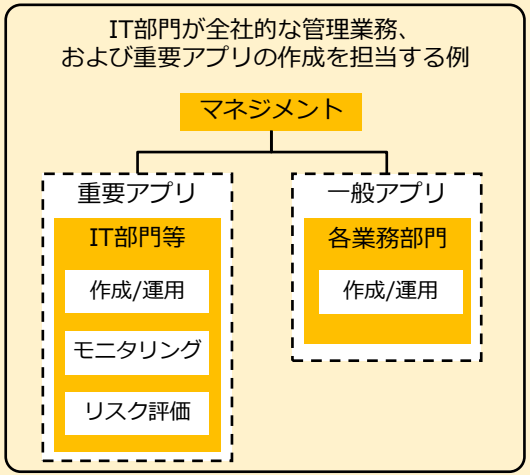
分散管理 ⟷ **中間** ⟷ **集中管理**

- 人材育成、アプリの作成/運用、リスク管理など各種管理を業務部門それぞれで対応する

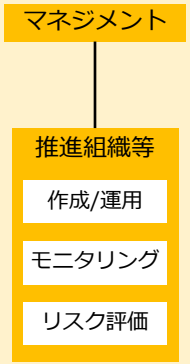


- アプリのモニタリングやリスク管理など、各種管理における特定の管理について推進組織などが集中的に管理を行う
- リスクに応じて管理体制を分離するなど、分散型をベースにしながら一部について集中管理を行う





- 人材育成、アプリの作成/運用、リスク管理など各種管理を推進部門やIT部門などの単一の部門で対応する



kintone

3.3.主な対応策(2/5) -人材育成-

kintoneにおける人材育成は、kintoneそれ自体に対する教育は勿論のこと、本資料で紹介するガバナンスに対する教育も肝要であると考えられます。特に推進組織担当者や部内管理担当者の役割を担う人員に対しては、ガバナンスに対する教育は必須のものとして考えることが望ましいです。

教育内容

kintoneに関する教育

【目的】

kintoneに関する知見を高めることにより、**kintoneを用いた業務改善スキル**を向上させる。

【教育の方向性及び例】

- kintoneの基本知識
- 業務の要件に合わせたkintoneアプリの作成方法
- kintoneプラグインを用いた開発方法
- 業務の変化に合わせたアプリのメンテナンス方法

ガバナンスに関する教育

【目的】

ガバナンスに関する知見を高めることにより、**kintoneガバナンスを実行する担い手**となる。

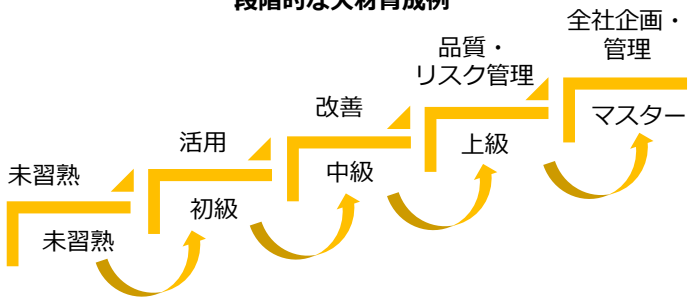
【教育の方向性及び例】

- ITガバナンスの全体像
- アプリのリスク評価の実施方法
- ガバナンスの実施にあたり利用可能なkintoneの機能の理解
- 自社のkintoneガバナンスに関する理解

教育の実施にあたり検討すべきポイント

- kintone推進にあたっての組織、及び組織における各人員の役割と、教育の方針をリンクさせることが望ましい。
- 重要な役割については予め求められるスキルレベルを定義し、一定の教育水準に達した人員のみがその役割を担うことが出来るようにするといった、段階的な教育方針とすることも有効。

段階的な人材育成例



kintone

3.3.主な対応策(3/5) -権限管理-

kintoneにおける権限は、kintoneのプラットフォームに対して管理する権限と、作成された個別のアプリ内で管理する権限に大別されます。

	管理者などの種類	紐づく主要な権限	権限管理における推奨ポイント
プラットフォーム権限	cybozu.com共通管理者 システム管理者	**kintoneの主要な設定を全て変更可** アプリやスペースの作成権限の設定 利用機能の選択 利用できるプラグインの追加	• 非常に強力な権限であるため、推進組織やシステム部門など、**限られた人員に権限を限定すべき** • 上記以外の人員に権限を付与する場合は、恒常的な権限付与ではなく**貸出等による一時的な権限付与が望ましい**
	アプリ管理者	**作成されたアプリの以下を変更可** アプリ内のフィールド追加 アプリ内のアクセス権、通知設定	• 実質的にアプリの処理や内部のレコードを自由に操作できる権限であるため、高リスクのアプリについては推進組織やシステム部門など、**限られた人員に権限を限定すべき**
	スペース管理者	**作成されたスペースの以下を変更可** スペースの公開設定 スペース参加メンバーの追加 スペースの削除	• スペース管理による分離（P.26参照）を実現している場合は、推進組織やシステム部門など、**限られた人員に権限を限定すべき**
個別アプリ権限	アプリのアクセス権	**個別に以下の権限を設定可** (1)レコード閲覧　(2)レコード追加 (3)レコード編集　(4)レコード削除 (5)アプリ管理　(6)ファイル読み込み (7)ファイル書き出し	• レコードの追加/編集/削除権限は、**業務上の必要性を有する人員に権限を限定すべき** • 個人情報を格納している場合は、レコード閲覧権限含め**業務上の必要性を有する人員に権限を限定すべき**

3.3.主な対応策(4/5) -ログ管理-

kintoneは、ユーザーの操作ログを監査ログとして取得しています。アプリやデータに対する意図しない操作の有無などの確認が必要な際に、当該ログを利用することが可能です。また、モニタリングのコントロールが求められる場合においても、ログを活用したモニタリングの検討が行えます。

監査ログの取得方法

Cybozu.com共通管理者メニューの「監査ログ」>「閲覧とダウンロード」から遷移する以下の画面で出力可能

主要な監査ログ	監査ログの活用例
アプリの作成/削除	**アプリのモニタリング** 申請なしに作成されたアプリの有無の確認
アプリ/レコードへの アクセス権の変更	**アクセス権のモニタリング** 意図しないアプリ/レコードへのアクセスが付与されていないことの確認
レコードの書き出し/削除	**レコードのモニタリング** 機密性が高いレコードについて、意図しない操作が実施されていないことの確認
プラグインのインストール	**プラグインのモニタリング** 認可したプラグイン以外が利用されていないことの確認

3.3.主な対応策(5/5) -複数領域での利用-

１企業内で複数の利用領域にまたがり利用する場合に、**スペース分離により管理を分けることも可能**です。しかし、スペース分離での管理を行う場合はシステム上分離が強制できないため、リスク低減のためには事後的なモニタリング等のコントロールの実施が必要となります。

スペースを分離し管理を分ける場合の例

アプリ作成時のリスク評価、及び、リスクに応じたアプリのスペース所属をルール上規定する

▼

同一サブドメイン内で、スペース機能を使って論理的にアプリを分離する

- **高リスクスペース** ▶ 高レベルのガバナンスを実施する
- **低リスクスペース** ▶ 一部緩和した運用を行いつつ、モニタリングによってルール無視の運用を防止する

【参考】スペース分離した場合のガバナンス例

スペースのガバナンス方針	具体的なコントロールのポイント
高レベルのガバナンスを実施する	全てのカテゴリに対して高レベルのコントロールを整備/運用する。 • 厳格な作成/変更管理プロセス 　• アプリ作成前の事前申請やテスト 　• 変更に対するモニタリング等 • 厳格なアプリ内の権限管理 　• 職務分掌に基づく権限設定 　• 権限付与時の事前承認 　• 定期的な棚卸し等
一部緩和した運用を行いつつ、モニタリングによってルール無視の運用を防止する	一部のカテゴリに対しては効率性の観点からコントロールの緩和を検討する。 • 自由なアプリの作成/変更を容認 • 自由なアプリ内の権限設定を容認 • 定期的なアプリ棚卸しにより、ルールを逸脱した利用がないかをモニタリング

【４】

リスクおよびコントロール例

4.1.リスク評価、管理（1/2）

項目	リスクの概要	リスクに対応するコントロールのポイント
アプリ重要度、リスクの評価	・利用企業の想定しない高リスクエリアにおいてkintoneが利用されることにより、情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・アプリの作成にあたり、リスクを評価するプロセスを整備する。 ・アプリのリスクを判断するための判断基準を設ける。
		・アプリ作成者は、アプリを作成する際に事前申請を行う。申請を受けた部署（推進組織等）は、アプリの作成難易度や使用するデータの重要性等を総合的に判断し、リスクを評価する。 ※リスク定義や判断において、業務部門（アプリ作成部門）以外の関与は組織・体制の観点と併せて検討を行う。
		・作成時及び運用時にリスクに応じた管理ができるように、リスクが高いアプリを特定できるようにする。 **＜kintone機能の活用＞** 「kintoneアプリ管理」アプリ（kintoneアプリストア）の利用
アプリ管理・作成ルールの整備	・リスクに応じて求められる管理・作成が行われないことに起因して、情報漏洩・法律・規制の逸脱、および要件を満たさないアプリが発生するリスク ・リスクに応じたルールとなっておらず、過剰なルールによってkintoneの利点が失われるリスク	・利用企業に応じて想定されるアプリのリスクに応じてアプリの作成/管理ルールを整備する。 ※全社にて同一のルールのみでなく、リスクに応じたルールの適用範囲の検討を行う。 ※リスクに応じて、業務部門（アプリ作成部門）以外が関与するかどうかは組織・体制の観点と併せて検討を行う。
アプリの作成権限の管理	・利用企業の想定していない人物にアプリの作成権限が付与されることにより、情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・必要に応じてアプリの作成権限を一部の従業員のみに付与する。 ・スペースを利用したアプリ管理のルールを整備する。 **＜kintone機能の活用＞** スペース機能の活用
		・アプリ作成者が、プラグインを利用したりJavaScript等のカスタマイズをしたい場合は、cybozu.com共通管理者またはシステム管理者に申請を行う。 ・cybozu.com共通管理者またはシステム管理者は申請内容を確認し、適用可否を判断した上で、利用を許可する。

4.1.リスク評価、管理（2/2）

項目	リスクの概要	リスクに対応するコントロールのポイント
各種法令・内部統制・コンプライアンス対応	・利用企業の想定しない高リスクエリアにおいてkintoneが利用されることにより、情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・各種法令・内部統制・コンプライアンスにあたって要求される事項を認識し、アプリ作成ルールやアプリ管理方法を整備する。 ※個社ごとに求められる要件に応じて細分化が必要
導入効果/コストの確認	・kintoneの導入効果が定量的に把握されておらず、当初設定した戦略に対する効果が十分でない場合の対処が行われないリスク。	・kintoneの導入に際してKPIを設定し、定期的に達成状況を確認する。アカウントの状況についても確認し費用対効果についても確認する。
アプリ作成状況の確認	・kintone利用戦略に沿わない利用がされているリスク	・作成されたアプリの一覧及びプラグインの一覧を定期的に出力し、推進組織が把握していない高リスクアプリの作成や、管理ルールとの不整合がないかの棚卸を行う。 ※どの観点までモニタリングを行うか（kintone基盤の設定・権限、アプリの要件・設定、アプリ権限、取扱いデータ、データの操作等）については、アプリのリスク評価に応じて検討を実施する。 **＜kintone機能の活用＞** アプリ一覧の出力機能
アプリ利用状況の確認	・kintone利用戦略に沿わない利用がされているリスク ・kintoneの利用が最適化されておらず、設定した目的が達成されていない場合、または、運用費用が適切でない場合に、対処されないリスク	・作成されたアプリの一覧及びプラグインの一覧を定期的に出力し、推進組織が把握していない高リスクアプリの作成や、管理ルールとの不整合がないかの棚卸を行う。 - アプリの把握　：　アプリ一覧および最終更新日等の把握 - 利用状況の把握　：　アプリのレコード数の把握 **＜kintone機能の活用＞** アプリ一覧の出力機能

4.2.開発・変更、運用（1/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
要件定義・設計	・要求する機能を完全に正確に提供できないアプリが作成されるリスク ・情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・リスクレベルが高いアプリの作成にあたっては、要件定義、設計資料の作成を行う。 ※ただし、kintoneのアプリ作成は通常のシステム開発よりも、利用範囲、影響範囲、開発規模が限定的な場合もあるため、通常のシステム開発より簡易的なもので許容可能だと考えられる。そのため、ユーザー自身で作成し、ユーザー自身で利用するアプリなど、対外的な影響有無や、後続の業務プロセス上のコントロール有無によっては、割愛することも検討する。「アプリ管理・作成ルールの整備」にて会社におけるkintoneの利用戦略・方針に応じて検討を行う。
		・アプリ作成者は、アプリを作成する際に事前申請を行う。申請を受けた部署（推進組織等）は、実現したい要件がkintoneで満たせるかどうかを以下の観点で評価し、アプリ作成可否を判断する。 - アプリの利用目的 - 使用するデータの種別 - 想定されるデータ量（レコード数、フィールド数） - 処理の複雑度（条件分岐の量等） - 想定されるトランザクション量（API含めたアクセス数）
開発	・要求する機能を完全に正確に提供できないアプリが作成されるリスク（性能に関わる要件を含む） ・情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・難易度の高いJavaScriptカスタマイズやプラグインを利用する場合には、その開発手順を整備する。また、外部システムと連携する場合には、その開発手順等を整備する。
テスト	・要求する機能を完全に正確に提供できないアプリが作成されるリスク ・情報漏洩・法律・規制の逸脱につながり得るアプリが作成されるリスク	・アプリ作成者は、kintoneの「アプリの動作テスト」機能を利用して、アプリを公開する前に動作確認する。 ※アプリのリスクや複雑性に応じて「アプリの動作テスト」機能を利用するだけではなく、別途テスト環境を準備する必要があるか、検討する。 ・テスト環境に利用するデータは、個人情報や機密情報などの重要情報を取り扱わない。また、テスト環境にデータを残さない。
		・高リスクアプリについては、アプリ作成者による機能テストに加えて、アプリ作成部門/推進組織等のチェックを行う。

4.2.開発・変更、運用（2/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
リリース管理	・リスクレベルが高いが未承認のアプリを業務に使用し、業務に影響を及ぼすリスク ・未完成のアプリのリリースや、開発におけるデグレーションの発生が、業務に影響を及ぼすリスク	・リリース手順及び利用者周知手順を整備する。
		・リスクレベルの高いアプリについては、リリース時にアプリ作成部門/推進組織等のリリース確認を実施する。 ・スペースに所属しないアプリの作成を許可しない ・kintoneのスペース機能を活用したリリース管理 **＜kintone機能の活用＞** スペース機能の活用 https://kintone.cybozu.co.jp/update/main/2021-11.html#point2 ※「新機能A、新機能Bを組み合わせた利用例」に記載の通り
変更手続きの整備	・アプリの誤った変更、意図しない変更により、要件通りにアプリが動作せず業務に影響を及ぼすリスク。 ・外部連携等により他システムの変更による影響を受ける場合、他システムの機能変更から発生する修正対応が漏れ、アプリの動作に影響を及ぼすリスク。	・アプリの変更手順を整備する。 - アプリの種類や外部連携、プラグインなどの状況から、重点的に管理すべきアプリを識別しておく - 重点的に管理すべきアプリとそれ以外のアプリでの差異について明確にしておく - アプリ管理権限を誰に付与するのかを検討する **＜kintone機能の活用＞** アプリ管理権限の設定
		・定期的に監査ログを出力し、意図しないアプリへの変更が発生していないことを確認する。 ※重要かつ複雑な処理ロジックを含む変更難度の高いアプリ、JSOXなどの内部統制の対象となるアプリなど、アプリのリスクに応じて対応を検討する **＜kintone機能の活用＞** 監査ログの利用

4.2.開発・変更、運用（3/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
アプリの運用管理	・アプリ作成後にアプリ管理者が異動や退職し、アプリ管理者が曖昧となった結果、アプリの維持管理が行われないリスク ※アプリ作成後の野良アプリの発生のリスク	・アプリの運用単位（部門・個人）およびアプリ管理ルールを整備する。 - スペース管理ルール - アプリ管理ルール（命名規則、アプリ管理者、アプリ数の管理、ステータス等） ・アプリ管理者の定義についてルールを整備する。 ・アプリ管理者の異動、退職時のアプリの維持管理ルールを整備する。 ・定期的なアプリ棚卸時にアプリ管理者を再確認する。
トラブル対応	・発生した障害が解消されず、アプリまたはレコードの完全性/可用性が侵害されるリスク ※障害は、カスタマイズで設定したJavaScriptやAPIに問題がある、ユーザーが利用している端末やブラウザ側に依存する現象など	・アプリ障害発生時の対応・支援体制、及び手順を整備する。 ・JavaScriptやAPIなどの利用時による、ローコード領域における障害検知について必要性の検討および対応する仕組みを整備する。
バックアップ・リストア	・アプリでの誤った操作、意図しない操作により、アプリ/レコードが書き換えられる、または削除され、アプリ設計およびデータの完全性、可用性が侵害されるリスク ※想定するリスクはkintone基盤でのデータ喪失のリスクではなく、アプリ上のユーザー操作による誤ったデータ操作に対するリスクを想定	・アプリ設定やデータを保全するため、必要に応じてバックアップ（手動でのレコードの書き出し）およびリストア手順の確認を実施する。
業務継続	・アプリが利用できないことにより業務が継続できなくなるリスク	・アプリが利用できない場合への対応手順を整備する。

4.3.アプリとデータアクセス（1/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
セキュリティ管理	・意図しないユーザーがcybozu.com及びkintoneにアクセスしてしまうリスク	・自社に求められるセキュリティレベルを考慮し、各種セキュリティに対する要件を整備する。
		・cybozu.comへのログインにあたり、求められる認証形態を確立し、整備する。
		・cybozu.com共通管理者やシステム管理者といった高権限アカウントについては、2要素認証等のセキュアな認証方法を検討する。
		・自社のパスワードポリシーを考慮し、cybozu.comへのログインにあたって求められるパスワードポリシーを設定する。

4.3.アプリとデータアクセス（2/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
ツール権限管理	・意図しないユーザーがkintoneにアクセスしてしまうリスク	・cybozu.com共通管理者は、定期的にkintoneの「ユーザー」及び「ユーザーの利用サービス」情報を書き出すことでユーザーの一覧を取得し、退職や異動等による不要なユーザーが存在していないかどうかを棚卸する。
	・意図しないユーザーが高権限アカウントにアクセスしてしまうリスク	・デフォルトの高権限アカウント（Administrator）について、業務上の必要性に基づき使用する場合を除いて、アカウントを停止する。
		・cybozu.com共通管理者、及びシステム管理者については、保有するユーザーを業務上の必要性が認められる最低限に限定し、退職や異動等の事象が発生した場合は速やかに権限をはく奪する。
個別アプリ権限管理	・意図しないユーザーが機密性の高いアプリにアクセスしてしまうリスク	・機密性の高い情報を保持するアプリについては、業務上の必要性に基づき、各ユーザーの権限は必要最小限にとどめる。
		・機密性の高い情報を保持するアプリについては、定期的に棚卸を行い、各ユーザーにとって不要な権限を削除する。
ログ管理	・重要操作を事後的に確かめることが出来ずその真正性が担保されないリスク	・重要操作について、ログを取得する。 ・ログについて社内外から求められるログ保管の要件に応じて保管期間を設定する。 ※ログのモニタリングについては、アプリの変更管理、データガバナンス、モニタリングの観点において必要性を検討し対応を実施する

4.3.アプリとデータアクセス（3/3）

項目	リスクの概要	リスクに対応するコントロールのポイント
データガバナンス	・意図しないレコードの変更により、レコードまたはアプリの完全性/可用性が侵害されるリスク ・意図しないレコードの閲覧により、レコードの機密性が侵害されるリスク	・重要データが登録されているアプリを特定する。
		・重要データが登録されているアプリの場合、業務上の必要性に基づき、アクセス権の付与は必要最小限に留める。 **＜kintone機能の活用＞** アプリのアクセス権、レコードのアクセス権、フィールドのアクセス権限
	・意図しないレコードの変更により、レコードまたはアプリの完全性/可用性が侵害されるリスク	・不正なデータ変更を予防及び発見するための対応策を整備する。 ・データを修整する際の手順について、整備する。
	・同じマスターデータなどが乱立し、データの正確性が阻害されるリスク	・マスターデータを共有する仕組みを整備する。 ・マスターデータが登録されているアプリの管理・運用ルールを整備する。

お問い合わせ先
サイボウズ株式会社
kintone Enterprise Circle 運営担当
kintone-ep@cybozu.co.jp