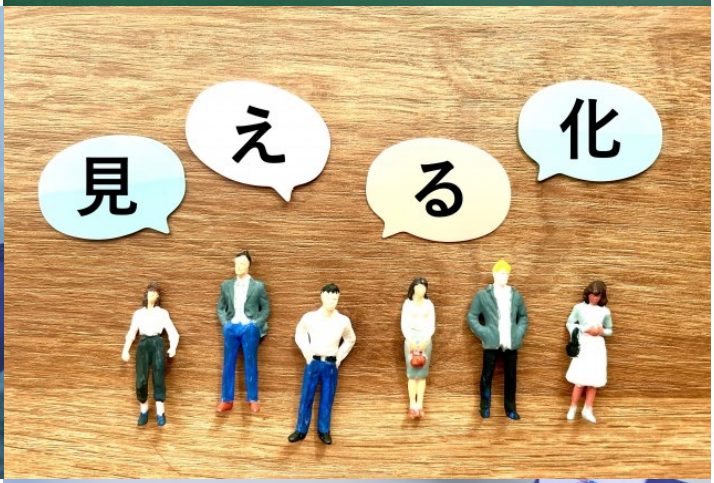
自治体様のデジタル化に係る支援サービスのご紹介

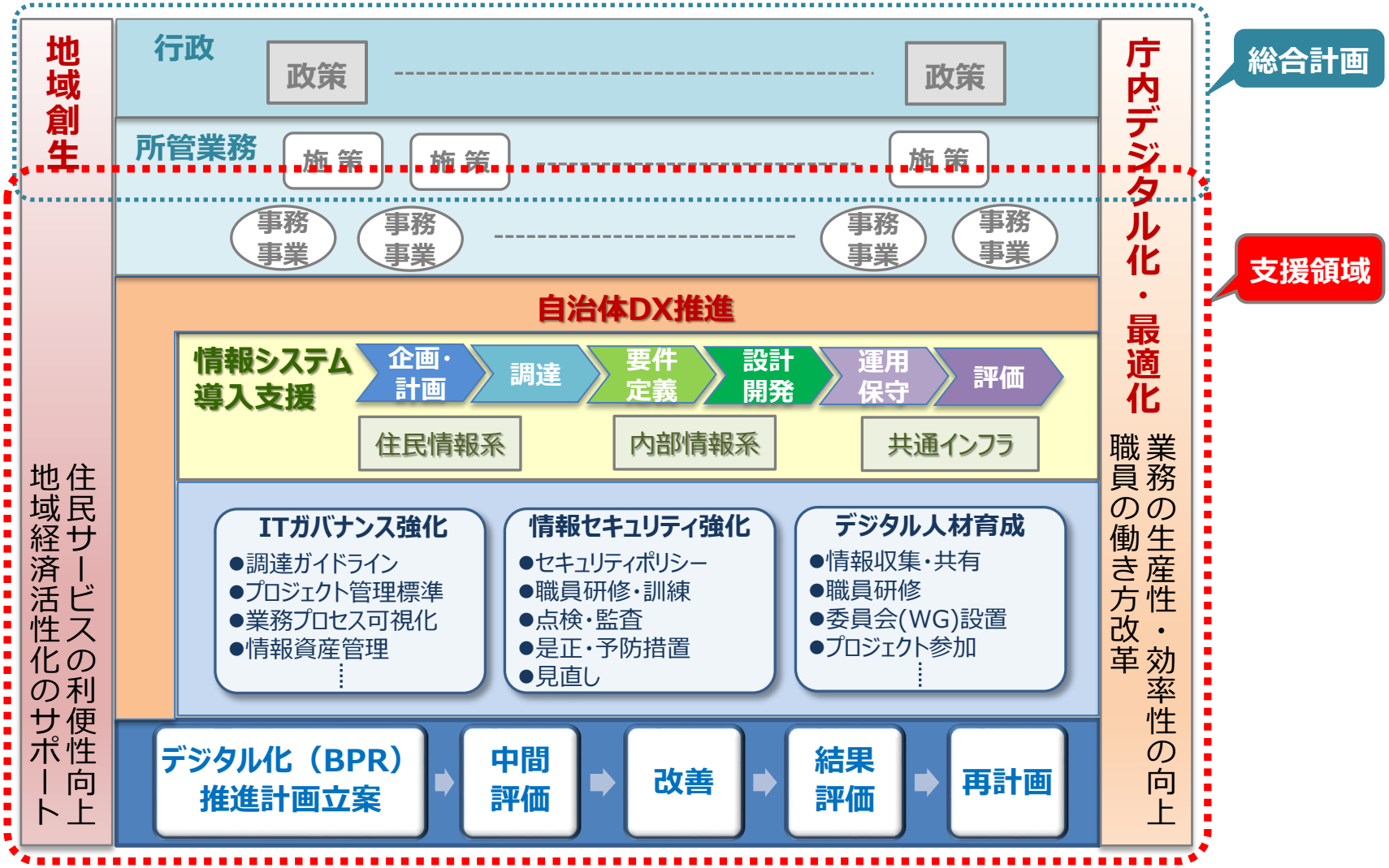


エスクリブ株式会社

SCriv

エスクリブ株式会社の業務概要

自治体庁内業務のデジタル化による業務改善、ITガバナンス力向上、情報セキュリティ対策強化、またデジタル人材育成等のご支援をさせて頂いております。



1. 最適な「デジタル化・IT調達」に関する支援

【関連事業の実績（直近5年）】
- 宮城県仙台市（令和元年度、令和2年度、令和4年度）
- 青森県六ヶ所村（令和3年度～令和5年度）
- 青森県風間浦村（令和3年度～令和5年度）

調査シートやヒアリングにより現場の業務内容と課題を整理

情報化計画書の作成

事例やデジタルソリューション等に関する情報を収集

RFIの実施

ベンダーとの認識齟齬をなくし、適正な費用で調達を行うための準備

RFIによるベンダーからの意見や質問への回答を整理

ベンダーから提示された見積を精査し、システムやサービスの機能・性能等に過不足がないか、適正な費用であるかを確認

仕様書に盛り込むべき情報を引き出し取りまとめ、調達方式や委託範囲（内容）等を具体化

ベンダーと折衝し、過剰な費用は圧縮

仕様（案）の作成

ブラッシュアップし、調達実行

2. DX推進に向けた業務改革（BPR）に関する支援

【関連事業の実績（直近5年）】
- 青森県六ヶ所村（令和4年度）
- 秋田県鹿角市（令和4年度～令和5年度）

業務改革（BPR）推進ステップ

【アンケート調査】
担当業務、庁内共通業務、住民サービスに係る問題について調査。

【重要問題選定】
アンケート調査結果から解決効果の高い重要な問題を選定。

【課題設定】
重要問題の原因を分析し、根本的な原因を課題として設定（ワークショップで行う場合あり）。

課題数により優先課題を抽出

※DXに関するWGまたはPJチーム等が組織されている場合は意見交換を行った内容を実施計画書へ反映します。

【解決の方向性検討】
課題対策の方向性をヒアリングを通して職員と共に検討。

【具体策提案】
課題解決に役立つデジタルツールを含めた課題解決に向けた具体策を提案。

※ **【実施計画書作成】業務改革（BPR）実施計画書にて個別プロジェクトを提示。**

スケジュールに従いプロジェクト開始

プロジェクトの例	窓口改革（書かない窓口、電子申請等、窓口ナビ、ワンストップ）、AI-OCR・RPA、電子契約等の導入による業務効率化、チャットボット導入による負担軽減 等

3. 業務改革（BPR）推進人材育成研修

【関連事業の実績（直近5年）】
- 青森県六ヶ所村（令和4年度）
- 秋田県鹿角市（令和4年度）

研修概要の事例

1	目標	業務改革をリードできる人材を育成する。
2	CSF（目標達成のための重要要因）	• 業務改革の実施に向けたモチベーションが促される。 • 課題解決や新たな価値をもたらす業務改革を進めるプロセス及びノウハウを習得する。 • アジャイル型のプロジェクトの推進をリードできるスキルを習得する。
3	受講効果	• 業務改革を理解し、実行するモチベーションが促される。 • 業務改革推進プロセスを習得する。 • アジャイル型のDXプロジェクトの推進方法を習得する。
4	研修概要	✓DX及び業務改革の解説と事例紹介（講義、動画視聴等） ✓業務改革の実践（講義、業務上の課題解決の方向性をグループワークにより検討、業務フロー作成演習） ✓アジャイル型DXプロジェクトの進め方（講義、仮想プロジェクトの推進をグループワークにより体験）
5	実施スケジュール	4.5時間／日の研修を2日間で実施（合計9.0時間） ※カリキュラムを調整し、研修時間の増減は可能
6	実施形態	原則、集合研修

4. 情報セキュリティ対策の強化に関する支援

情報セキュリティ対策を強化すべく以下の施策に係る支援を行います。

- 情報セキュリティポリシー、情報セキュリティ実施手順、ハンドブックの策定・見直し
- 職員研修（アンケート分析等を含む）
- 標的型メール攻撃やインシデント対応に関する訓練
- CSIRTの構築、運用
- 自主点検（職員及び課室等の部署）、外部監査
- マネジメントレビュー（情報セキュリティ委員会等での助言、意見表明等）
- 情報セキュリティに関する各種助言・提案（提言）
- Webサイト、Webアプリケーションの脆弱性診断

【関連事業の実績（直近5年）】
- 宮城県富谷市（令和元年度～令和6年度）
- 宮城県仙台市（令和元年度～令和2年度）
- 長野県軽井沢町（令和元年度）
- 青森県六ヶ所村（令和4年度～令和5年度）
- 秋田県鹿角市（令和4年度～令和5年度）

※ 自治体様により支援内容は異なります。

【恒常的なセキュリティ対策が求められる理由とその対応】

- デジタル化が進む一方、ミスや無知、また複雑化かつ高度化した悪意を持った攻撃への対策を十分に行っていないと事故につながりかねません。⇒ セキュリティポリシーの策定及び見直しを行い、その周知を含めた定期的な職員研修と訓練を実施する。
- 職員個人や課室等の部署により、情報セキュリティに対する意識と対応が異なることは事故が起きる要因となるため、そのレベルを合わせ、向上させる必要があります。⇒ 毎年、自主点検及び情報セキュリティ監査を行い、改善対策を行う環境を整える。

【弊社の情報セキュリティ対策に関する考え方】

日々新たな情報セキュリティに関する脅威と脆弱性が発生また検出されることから、セキュリティ管理レベルを常に向上させなければなりません。そのためには、適切にセキュリティポリシーを見直し、これに基づいた運用を行い、職員個人や課室等の部署のセキュリティに対する意識と対応を点検と監査にて可視化し、改善を施すPDCAサイクルを回す必要があります。

弊社は、職員の負担を少しでも減らし、効率的で有効なセキュリティ対策を行うことを推奨しております。従って、すべての職員と課室等の部署に画一的な対策を求めるのではなく、「リスクベースに基づいた対策実施」を基本的な考え方としています。