

# 2024年度 分科会 募集テーマ

活動期間 2024年2月～2025年2月  
(全国大会参加の場合は3月末まで)

ここに書かれている研究概要や活動ポイントはあくまでも案で、実際の研究内容やどこに焦点を当てるかは分科会で決めていただきます。

開催地区 東 東日本地区(東京) 中 中日本地区(名古屋) 西 西日本地区(大阪)

カテゴリ	分科会テーマ	開催地区	開催概要	活動ポイント
経営	共創を通じた 新ビジネス創出の プロセスを学ぶ ～共創DXケーススタディ 編～	東 中 西	異文化・異業種の企業がタイアップし、最先端のIT技術を使ってビジネスモデルの改革につながる新サービスを生み出す、というようなことが夢ではなくなってきました。特にITに着目し、各社の強みとITを組み合わせるとどのような新サービスが生まれるのか、ケーススタディを研究し、共創DXを生み出すプロセスを導き出します。分科会活動の中で、参加企業同士または仮想企業の共創で新ビジネスを創造(想像)するのも面白いかもしれません。	<ul style="list-style-type: none"> <li>共創によるDXのケーススタディ</li> <li>共創を成功させる企業の条件やポイント</li> <li>新ビジネスの創出プロセスとは</li> </ul>
育成	DX時代の人財戦略 ～デジタル人財という言葉 の落とし穴～	東 中 西	DX実現のためにデジタル人財の育成に取り組む企業が多いものの、実態はデジタルスキルの習得に片寄っているのではないのでしょうか。またそのスキルを獲得しても発揮する場がないという声も聞かれます。一方、新たな価値創造(DX)にはゼロからの発想力やチャレンジ精神などのソフトスキルや業務を良く知るアナログ人財も重要です。この分科会では、DX実現のために必要な人物像を改めて考え、その育成方法を検討します。全社員がデジタル人財であるべきか、アナログ人財とデジタル人財の融合は?などを検討し、「DX実現に本当に必要な人財とは?」の答えを導き出します。	<ul style="list-style-type: none"> <li>DX実現に必要な人物像の明確化</li> <li>求められる人財の育成方法</li> <li>リスクリングのためのスキルの可視化</li> </ul>
組織	働き方改革から見た 「コロナ禍の総括」 ～維持すること、 変えること～	東 中 西	コロナ禍により、それ以前はまだまだ先と思われていたテレワークなどの働き方改革が一気に推し進められました。コロナはいわば非常事態でしたが、平時に戻りつつある今改めて、コロナ以前に戻すこと/今の状態を維持すること/ここからさらに変えていくことは何かを、特にITの利活用の側面から整理し、今後目指すべき「働き方改革」の姿を提示します。	<ul style="list-style-type: none"> <li>働き方改革から見たコロナ禍の功罪</li> <li>戻すこと/維持すること/変えることの整理</li> <li>働き方改革のあるべき姿とITの可能性</li> </ul>
組織	DX推進のための 組織のあり方 ～DX推進のための 組織変革～	東 中 西	DX推進を担うデジタル人財の育成が各社の課題になっていますが、組織はこのままで良いのでしょうか。ビジネスの変革(DX)過程では、システム開発におけるアジャイルのようにトライアンドエラーを素早く回す必要があります。ではアジャイル型アプローチが可能な組織とはどのようなものなのでしょうか。企画・開発・製造などの一連のプロセス、さらにはユーザー部門、IT部門、ベンダーなどが一貫通貫でDXを推進できるようにするためには、どのような組織への変革が必要でしょうか。本分科会ではDX推進を組織面から研究します。	<ul style="list-style-type: none"> <li>従来型組織とアジャイル型組織との違い</li> <li>アジャイル型組織の体制、役割、責任範囲</li> <li>組織変革に必要なこと</li> </ul>
組織	ベンダーフリーを 目指して ～ベンダーロックインを 打ち破れ～	東 中 西	ベンダーロックインはDX推進の足かせとも言われています。この分科会では、ベンダーロックインから脱却するためにはどうすればいいのかが研究されます。ベンダーに依存していることによる弊害、その依存はどこに原因があるのか、脱却する方法、および、ロックインを予防する方法を、参加企業および、各社の事例をもとに導き出します。	<ul style="list-style-type: none"> <li>ベンダーロックインの弊害</li> <li>ベンダーフリーになるためには</li> <li>ベンダーロックインを予防するためには</li> </ul>
プロジェクト管理	PMBOK7の実践 ～PMBOK7を学んで アジャイル開発を 推進しよう～	東 中 西	PMBOK第7版(PMBOK7)は、ウォーターフォールから「アジャイル型」プロジェクトに大きく舵を切ったと言われています。しかし、アジャイル開発が浸透しにくい日本ではまだまだ活用されていないのではないのでしょうか。本分科会では、PMBOK7をベースにアジャイル開発におけるプロジェクトマネジメントの体系を理解し、それを実践に移すためにはどうすべきかを考えます。不確実性の時代と言われる今こそ、王道のPMBOKを学び自社でアジャイル開発を推進してみたいかがでしょうか。	<ul style="list-style-type: none"> <li>PMBOK7の理解、どう変わったか</li> <li>アジャイル開発のためにPMBOK7をどう適用するか</li> <li>PMBOK7の実践</li> </ul>
情報活用	ビジネスに貢献する データ活用 ～様々なビジネスシーンで の活用～	東 中 西	企業では生産状況の見える化や売上分析といった直接的な企業活動で得られるデータ以外にも、勤怠管理やEXと呼ばれる従業員体験/満足度など幅広いデータが蓄積されています。これら未活用のデータを活用することで、例えば従業員のウェルビーイング(健康や生活の向上)に役立つかもしれません。この分科会では、ビジネス上の様々なシーンにおけるデータ活用の研究を通じて、ビジネス貢献につなげるためのデータ活用の指針を考えます。	<ul style="list-style-type: none"> <li>企業で収集されているデータ</li> <li>ビジネスシーンにおけるデータ活用事例</li> <li>ビジネスに貢献するデータ活用</li> </ul>

カテゴリ	分科会テーマ	開催地区	開催概要	活動ポイント
AI	企業は生成AIを どう活用すべきか ～生成AIを使った ビジネス変革～	東 中 西	急速に進化する生成AI。チャットや文書生成以外にも、画像/動画生成、プレゼン資料作成、自動コーディングなど様々な新サービスが提供されています。ビジネス利用を見越して社内データを生成AIで活用する模索も始まっています。一方で著作権侵害や、社内データの無断利用や流出が問題になっています。生成AIの各種サービスの調査、利用事例、課題整理を通じて、企業で生成AIをどう活用していくべきか、生成AIの活用で企業が変わるかを探ります。	<ul style="list-style-type: none"> <li>生成AIサービスと事例の調査</li> <li>生成AI活用の課題やガイドラインの検討</li> <li>生成AIがビジネスに与える影響</li> </ul> <p>※生成AI有償版サービスを利用する場合の当会の予算は、各分科会の活動予算と同様、年間5万円です。</p>
セキュリティ	サイバー攻撃および インシデント対策 ～DX推進の前に押さえる べき基本事項～	東 中 西	日本はサイバー攻撃の経験が少ないためか、セキュリティ分野での対応が遅れていると言われています。まずはサイバー攻撃を防ぐための基本的な対策を学ぶとともに、実際に攻撃された場合、いかに早くそれに気づき、どのような対策を取ればいいのかの基本事項を整理します。DX推進にもセキュリティ対策が不可欠と言われており、ユーザー部門の方も押さえておくべき基本事項です。	<ul style="list-style-type: none"> <li>サイバー攻撃対策</li> <li>サイバー攻撃者の心理を研究</li> <li>インシデント対策</li> </ul>
セキュリティ	SASEおよびSSEの 研究 ～サイバーセキュリティ・ フレームワーク～	東 中 西	企業の情報セキュリティで最近注目されているのが「SASE」(Secure Access Service Edge)や「SSE」(Secure Service Edge)です。ゼロトラストがセキュリティ全体に対する考え方なのに対し、ゼロトラストネットワークを実現するために、セキュリティ機能とネットワーク機能を一つのクラウドサービスに統合させるセキュリティフレームワークがSASEで、SASEのセキュリティ機能(CASBやSWGなどで構成)を担うのがSSEです。ゼロトラストから一歩具体化して、SASEやSSEのアーキテクチャやメリットを研究するとともに、従来のセキュリティ対策の違いや企業での活用を研究します。	<ul style="list-style-type: none"> <li>SASE/SSEの生まれた背景</li> <li>SASE/SSEのアーキテクチャやメリット</li> <li>従来のセキュリティ対策との違いや活用方法</li> </ul>
セキュリティ	サイバー攻撃手法の分析 と企業対策 ～戦え! 情報システム部。 敵を知り、己を知る～	東 中 西	企業や組織を狙うサイバー攻撃の手法は常に進化し、十分な対策を実施している企業でも次々と新たな被害が生まれています。本分科会ではサイバー攻撃の攻撃側から考え、様々な攻撃手法やビジネスモデルを学ぶとともに、その手法を熟知することで、企業が取るべきサイバー攻撃対策について研究します。	<ul style="list-style-type: none"> <li>サイバー攻撃手法の分析</li> <li>サイバー攻撃のビジネスモデル</li> <li>企業の攻撃対策</li> </ul>
システム開発	サーバーレス/ マイクロサービス を利用した基幹システム の刷新 ～変化に強いシステムに 生まれ変わるためには～	東 中 西	DX推進のためには、巨大なレガシー基幹システムを変化に強いシステムに刷新することが求められています。本分科会では、基幹システム刷新へのサーバーレス/マイクロサービス技術の適用やシステムの刷新手法について研究します。サーバーレス/マイクロサービス技術とは何か、なぜこれらの技術が求められているのかを学ぶことから始め、基幹システムの刷新にどう適用できるかを検討します。	<ul style="list-style-type: none"> <li>サーバーレス/マイクロサービスとは</li> <li>基幹システム刷新へ適用するための手法</li> <li>サーバーレス/マイクロサービスで刷新する際の勘所</li> </ul>
システム開発	ノーコード/ ローコード時代の システム開発 ～内製力を高めるために～	東 中 西	DX推進に向けたアジャイル開発のために、業務をよく知るユーザー部門による「ノーコード/ローコード開発」が本格化してきています。内製化が進む一方で、システム部門の管轄外で野放し状態での開発が行われるような問題も起きています。ユーザー部門によるノーコード/ローコードを使った開発を推進するにあたり、内製化のルールやガイドラインを策定することで、内製力の強化を目指します。	<ul style="list-style-type: none"> <li>ユーザー部門による内製化に向けてのルール整備</li> <li>ガバナンスの強化</li> <li>内製力を高めるための施策検討</li> </ul>
システム開発	システム開発自動化の 未来 ～どこまで自動化 できるか～	東 中 西	生成AIを利用した自動コーディング「Copilot」、テストスクリプトの生成、ドキュメント作成など、従来型のノーコード/ローコードツールだけでなく、システム開発を自動化するための仕組みや機能が、AIにより高度に発展してきています。これらの効果的な活用によって、システム開発はどこまで自動化できるのか。その未来像を探るとともに、自動化ツールの導入や自動化推進において気を付けるべきポイントを提示します。	<ul style="list-style-type: none"> <li>自動化ツールの現状(事例や適応分類)</li> <li>どこまで自動化できるか(未来像)</li> <li>自動化において気を付けるべきポイント</li> </ul>