- [x] Security Consulting
- [ ] Security Assessment
- [ ] Managed Security

三井物産セキュアディレクション株式会社

〒103-0013 東京都中央区日本橋人形町1丁目14番8号 JP水天宮前ビル6階
TEL：03-5649-1961（代表）

https://www.mbsd.jp/

Part No. CTS11-1001-2510

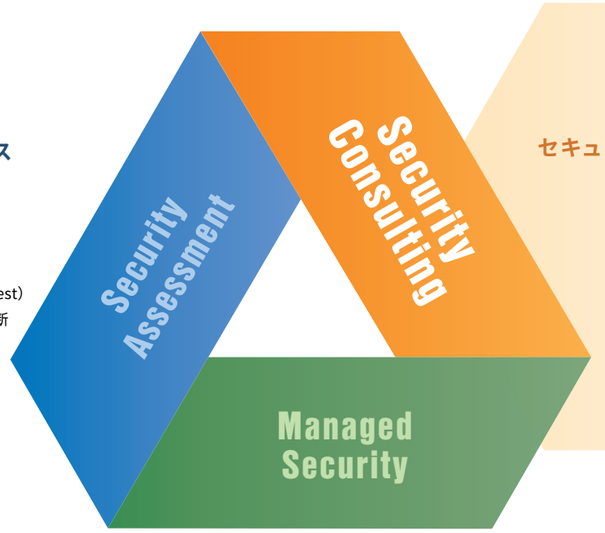
Security Consulting Service

セキュリティコンサルティングサービス

顧客課題に向き合い、深く現場と伴走する
個別最適なコンサル支援

Services

MBSDの事業は3サービスを軸として提供しています。



セキュリティ診断サービス

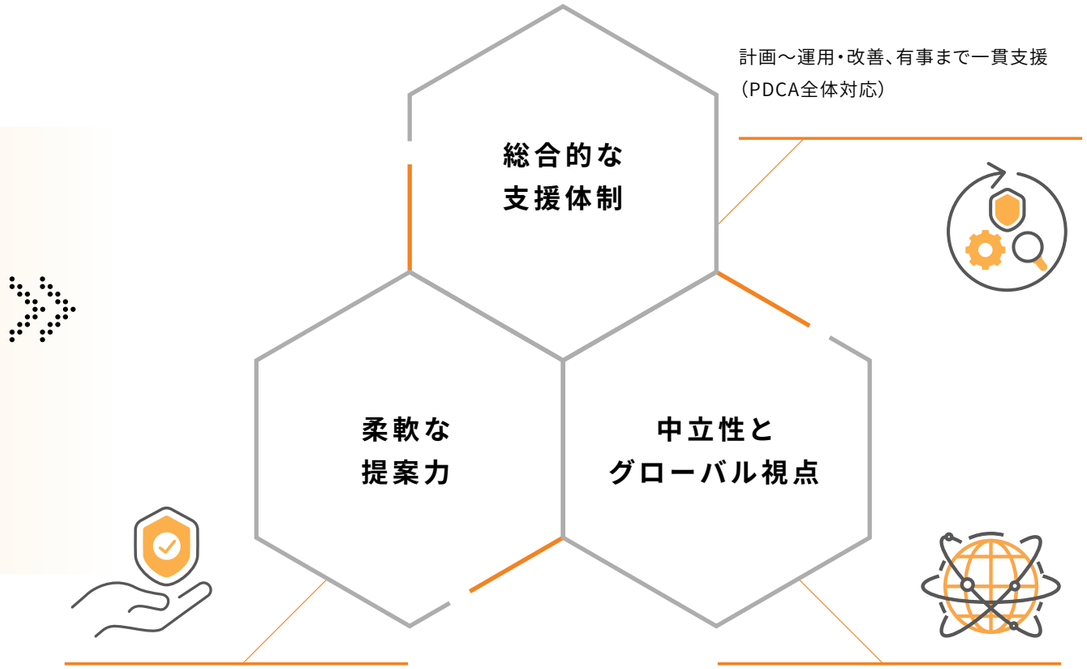
- Webアプリケーション診断
- ネットワーク診断
- スマホアプリ診断
- ペネトレーションテスト
- TLPT（Threat Led Penetration Test）
- AIシステムに対するセキュリティ診断
- 要塞化支援
- IoT診断
- ゲーム診断
- OT診断

セキュリティコンサルティングサービス

- リスクアセスメント
- セキュリティ組織運用支援
- セキュリティ戦略立案支援
- CSIRT構築・運用支援
- グループ・グローバル体制強化支援
- シンクタンクコンサルティング
- AIセキュリティ対策支援
- その他のサービス

セキュリティ監視サービス

- MBSD Managed Security Service（MBSD-SOC）
- Microsoftセキュリティ監視
- 統合ログ監視・Advanced SOC
- 統合ログ環境構築支援
- Security Force



計画～運用・改善、有事まで一貫支援
（PDCA全体対応）

組織規模・リソースに応じて、現実的で
最適な施策を提案

ベンダーフリーかつ世界最先端の情報に
基づいた提案

**この小冊子では、当社の具体的なソリューションを通じて、
貴社の成長を力強く支えるための
セキュリティコンサルティングサービスについて紹介します。**

Security Consulting Service

セキュリティ戦略から運用まで
企業の課題に寄り添う伴走型コンサルティング

デジタル化の進展に伴い、企業を取り巻くセキュリティリスクはますます高度化・多様化しています。クラウド利用やリモートワークの普及、AI・IoT導入が進む現在、従来の境界型防御だけではセキュリティを確保することが困難となり、経営層から現場に至るまで、組織全体での包括的な対策が不可欠です。

当社は、リスクアセスメントから組織体制の構築、規程整備、教育・演習、さらには運用・監査の支援までを網羅するコンサルティングサービスを提供しております。経験豊富なコンサルタントが、お客様の業務特性や事業環境を深く分析し、実効性の高い最適なセキュリティ強化プランを伴走型でご提案します。単なる評価や改善提案に留まらず、お客様の組織にセキュリティ体制が持続的に機能し、定着するまでを支援することで、企業の信頼性向上と着実な事業成長に貢献します。

Consulting Service Menu
セキュリティコンサルティングサービスメニュー

リスクアセスメント
- ベースライン・アプローチ
- リスクベース・アプローチ
- セキュリティ監査
- OTセキュリティ評価
- クラウドセキュリティ評価

リスクマネジメント
- サイバーBCP構築支援
- セキュリティポリシー・ガイドライン策定支援
- IoTセキュリティ対策支援
- AIセキュリティ対策支援
- クラウドセキュリティ対策支援

セキュリティ組織支援
- CSIRT組織構築支援
- CSIRT運用支援
- CSIRT成熟度評価支援
- セキュリティ戦略立案支援
- シフトレフト戦略支援
- グループ・グローバル体制強化支援
- セキュリティ人材育成
- サイバー演習・訓練支援
- セキュリティコンシェルジュサービス

シンクタンクコンサルティング

Service
セキュリティコンサルティングサービス

Features
コンサルティングサービスの特長

- ☑ 幅広い提供範囲（戦略から運用まで一気通貫）
- ☑ お客様視点で最適な提案（セキュリティ専業企業20年の実績と知見）
- ☑ 幅広いグローバルネットワーク（三井物産のグローバルネットワークを活用）
- ☑ 多彩な形態で支援が可能（訪問・常駐・リモート・ハイブリッド）

お客様の様々な課題に対して、現場に密着し着実な成果を実現

統制
- セキュリティ推進組織の整備（役割/責任/権限）
- サイバーセキュリティ戦略の立案
- ポリシー、規程、基準の策定、改訂
- グループ会社（国内/海外）管理
- サプライチェーンのリスク管理

識別
- 資産管理（管理漏れ、シャドーIT）
- リスクアセスメント手法、範囲、頻度
- 脆弱性の早期検出（シフトレフト化）
- 脆弱性情報取集、対象の確認（ASM活用）
- 脆弱性診断実施頻度、結果の管理

復旧
- サイバーBCP/BCM構築
- サービス/システム復旧手順の整備
- システム復旧テスト

防御
- ID管理（棚卸し、権限付与/削除）
- アクセス制御（マイクロセグメンテーション）
- セキュリティ教育内容、方法、効果測定
- 脆弱性対応（CVSS、KEV）
- セキュリティ対策ソリューション評価 、検証

対応
- CISRT構築、運営
- インシデント報告（関係者/外部機関）手順の整備
- （脅威毎）インシデント対応手順の整備
- デジタルフォレンジック体制準備
- サイバー訓練の実施

検知
- 監視範囲（外部脅威/内部脅威）、アラート設定、運用設計
- 継続的な監視の実現（SOC構築、SOC選定）
- 脅威インテリジェンスの活用

※NIST Cybersecurity Framework2.0より抜粋

リスクアセスメント

お客様の事業環境やセキュリティ成熟度に応じて、最適な評価アプローチをご提供します。国際規格や業界標準、そして豊富な専門知識を基に、リスクを正確に可視化し、お客様が取るべき具体的かつ効果的な対策の策定をご支援します。

01 ベースライン・アプローチ

SERVICE

国際規格（ISO/IEC 27001等）や業界標準といった、専門家の知見が体系化された「セキュリティ基準（ベースライン）」を用い、お客様の対策状況を客観的に評価する手法です。自社が達成すべきセキュリティレベルを明確にし、現状とのギャップを分析することで、取り組むべき課題の優先順位付けと、具体的な改善計画の策定を支援します。

02 リスクベース・アプローチ

SERVICE

お客様が保護すべき「情報資産」を起点に、個々の資産に潜む「脅威」と「脆弱性」を分析・評価する手法です。画一的な対策ではなく、事業への影響度が最も大きいリスクを特定し、限られたリソースを優先的に投下することで、セキュリティ投資の効果を最大化させます。

Service Delivery Process

サービス提供フロー

範囲の決定

- サービス内容のご説明
- アセスメント範囲の設定
- スケジュール調整

チェックシート記入

- チェックシートの記入（お客様）
- 内容QA受付

ヒアリング・現地調査

- 回答内容の精査および分析（必要に応じて追加質問）
- 現地調査による実態確認

分析

- ヒアリング結果の精査
- 既存資料の確認
- リスク分析
- リスク対応策検討

対策案立案・報告

- ヒアリング結果のまとめ
- 報告書作成

03 セキュリティ監査

SERVICE

お客様が導入済みのセキュリティ対策や社内ルールが、意図通りに機能しているか（有効性）、また国際規格（ISO/IEC 27001等）に準拠しているか（適合性）を、第三者の視点から客観的に検証・評価します。これにより、これまでの投資効果を証明するとともに、継続的な改善活動へと繋げます。

04 OTセキュリティ評価

SERVICE

工場やプラントで稼働する産業制御システム（OT）環境を対象に、現地調査やヒアリング、実践的な診断を通じて、システムやネットワークに潜むリスクを可視化します。国際規格（IEC 62443等）に基づき、事業や生産活動への影響度を考慮した最適な対策を提案し、評価から対策立案、運用まで一貫してご支援します。

05 クラウドセキュリティ評価

SERVICE

お客様のクラウド利用環境（IaaS/PaaS/SaaS）に対し、設定の不備や潜在的なリスクを専門家の視点で評価します。国際規格（ISO/IEC 27017等）やクラウド事業者が示すベストプラクティスに基づき、クラウド特有の脅威から情報資産を保護するための現実的かつ効果的な改善策をご提案します。

リスクマネジメント

現代社会において情報資産の保護は、企業の事業継続と信頼維持に不可欠です。近年では、標的型攻撃やランサムウェアなどのサイバー攻撃に加え、内部関係者による不正行為など、情報資産への脅威が日々巧妙化しています。このような攻撃や不正によってひとたび被害が発生すれば、経営に与える影響は甚大です。そのため、もはや事後的な対応だけで十分とは言えず、確かなリスクマネジメント体制の構築・運用が必須となっています。

進化するサイバー脅威に対応するため、サイバーBCP（事業継続計画）の構築支援や、実態に即したセキュリティポリシー・ガイドライン策定はもちろん、IoTやAI、クラウドといった最新技術を活用するビジネス環境にも即応した最適なセキュリティ施策をご提案いたします。お客様個々の業種や事業規模、ご要望に合わせてカスタマイズしたコンサルティングを通じて、堅牢で柔軟性のあるリスクマネジメント体制を実現し、レジリエンスと競争力を兼ね備えた持続的成長を力強く支援します。

01 サイバーBCP構築支援

サイバー攻撃がますます巧妙化・深刻化する現代、企業が事業を止めず信頼を守るための備えは、経営にとって不可欠です。豊富な経験と最新知見を活かし、サイバーリスクに強いBCP（事業継続計画）の策定から運用定着・継続的改善まで、一貫した支援を提供します。

Service Process

サイバーBCP構築支援のサービスプロセス

分析	重要業務の特定	設計	整備	訓練
●ビジネスやシステムの現状、組織体制の分析	●重要業務の特定と優先順位付け	●バックアップ／復旧体制や代替業務の設計	●サイバー攻撃発生後も重要業務を維持・復旧するための運用体制と連携ルールの整備	●訓練やガイドライン整備、最新脅威動向に応じた継続的な見直し

策定～運用の全工程を通じて「事業を止めない力」をともに築き、
貴社の信頼ある経営を徹底サポートします。

02 セキュリティポリシー・ガイドライン策定支援

最新の脅威動向や法規制、業界標準を踏まえ、実効性と運用しやすさを兼ね備えたポリシー・ガイドラインの策定を支援します。経営層や現場との対話を通じて課題を明確化し、策定から社内浸透・運用まで伴走することで、組織全体のセキュリティレベル向上を実現します。

03 IoTセキュリティ対策支援

IoT特有の脅威に対応し、機器・システムのライフサイクル全体で安全性を確保。脆弱性調査や多層対策、運用ルール整備、サプライチェーン管理やインシデント対応、教育・ガイドライン策定まで現場に即して伴走します。

04 AIセキュリティ対策支援

AI特有のリスクや倫理課題に対応し、設計・開発から運用・保守までライフサイクル全体で安全性を確保。改ざんや悪用リスク、推論結果の信頼性確保、情報漏洩防止、AI倫理・ガバナンスの対策、教育・ガイドライン策定まで現場に即して伴走します。

05 クラウドセキュリティ対策支援

クラウド環境のリスクや脆弱性を診断し、本当に守るべき資産と優先課題を明確化。アクセス管理や多要素認証、データ暗号化、バックアップ、リアルタイム監視、ポリシー策定や教育まで現場に即して伴走し、継続的な安全性確保を支援します。

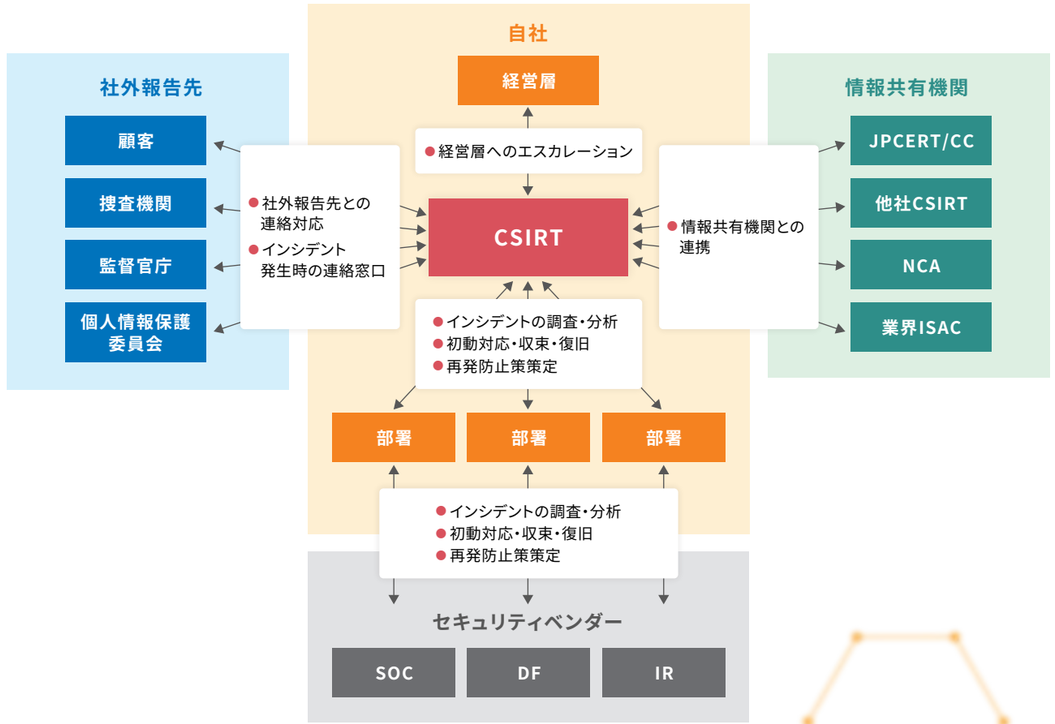
セキュリティ組織支援

ITの利活用が企業の収益性向上に不可欠となる一方、日々高度化・巧妙化するサイバーリスクは、経営における最重要課題の一つです。そのため、リスクに確りと備えるための組織体制や仕組みの構築が急務となっています。
当社は20年以上にわたり培ってきた経験・技術・実績を活かし、最新のサイバー攻撃から企業のあらゆる資産を守る組織体制の整備を、課題の可視化から改善策の提示、実装、運用まで一貫してサポートいたします。

01 CSIRT 組織構築支援 SERVICE

CSIRT新設や既存CSIRTの課題解消を目的に、組織体制や運用、手順・情報共有を分析し課題を可視化。役割明確化やチーム編成、マニュアル整備、関係部門・外部連携、演習・トレーニング、PDCA定着まで現場に即して伴走し、実効性あるセキュリティ組織の構築を支援します。

CSIRTの組織体制と役割分担の一例



02 CSIRT 運用支援 SERVICE

CSIRTの日常業務や対応プロセスを分析・改善し、初動対応や情報共有、標準化フロー、定期訓練、脅威情報活用まで現場に即して支援。外部SOC連携や運用ドキュメント見直し、組織横断情報共有基盤構築も含め、持続的かつ柔軟なCSIRT活動をサポートします。

03 CSIRT 成熟度評価支援 SERVICE

CSIRTの活動を第三者視点で定量・定性評価し、ガバナンス・体制・手順・技術・教育・情報共有を多角的に診断。課題や強化点を抽出し、短期・中長期で実践可能な改善策や段階的アクションプランを提案。自律的成長と脅威耐性の高いセキュリティ組織への変革を支援します。

Service Delivery Process
サービス提供フロー

セキュリティ組織支援

Other Services
その他サービス

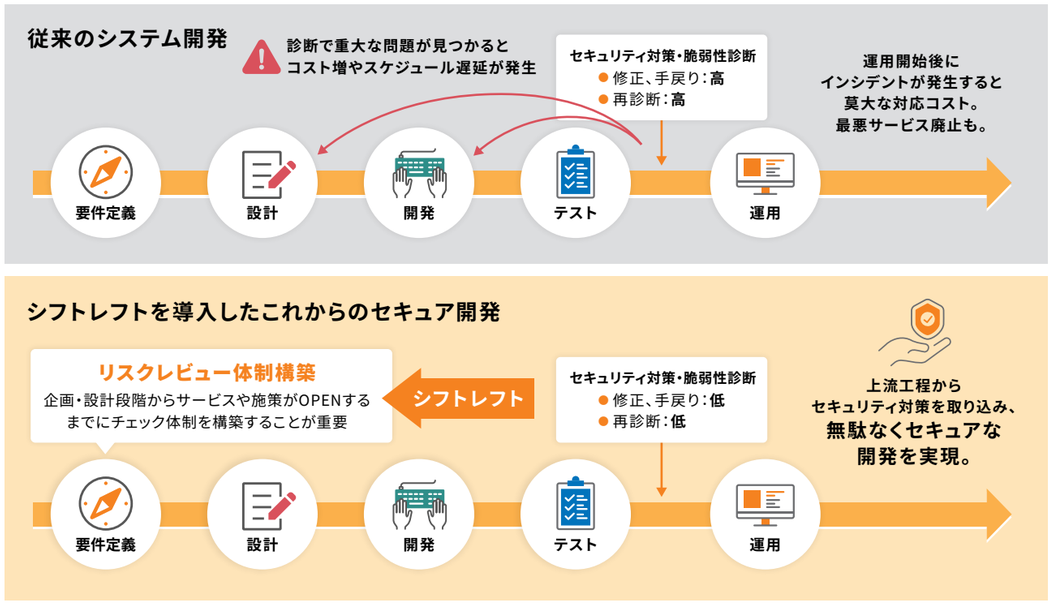
04 セキュリティ戦略立案支援 SERVICE

事業目標とリスク環境に基づき、専門知見と実績で最適なセキュリティ戦略を策定支援。現状分析から課題抽出、法規制や国際基準を踏まえたロードマップを提示。合意形成やKPI設定、進捗評価まで一貫して支援し、全社的な高度化と経営価値向上を実現します。

05 シフトレフト戦略支援 SERVICE

「シフトレフト」の思想に基づき、要件定義・設計・実装の各工程で脆弱性を早期発見し未然防止を支援。セキュア設計やコーディング指導、SAST/DAST導入など実践的に対応します。さらにDevSecOps体制の整備や教育、現場研修を通じて開発文化にセキュリティを根付かせ、スピードと品質を損なわず継続的な強化を実現します。

情報セキュリティを企画・設計段階から確保するための方策



06 サイバー演習・訓練支援 SERVICE

組織のニーズに応じた訓練プログラムを設計・提供。机上演習やハンズオンにより初動対応から復旧までを体験し、経営層・CSIRT・現場を巻き込んだ横断的訓練も可能です。訓練後は評価と改善提案を行い、定期開催や内容更新を通じてサイバー脅威に強い体制づくりを継続的に支援します。

07 セキュリティ人材育成 SERVICE

サイバーセキュリティ人材育成を支援し、目的や現状に応じた多様なカリキュラムを提供。基礎的なリテラシー教育から最新攻撃動向や脆弱性対策の技術研修、CSIRT・SOC運用に特化した実践プログラムまで幅広く対応し、専門性と実践力を備えた人材を育成します。

08 グループ・グローバル体制強化支援 SERVICE

グループ全体のセキュリティ強化を目指し、拠点や子会社の業務・成熟度・文化に応じた実効的支援を提供。現状評価や課題可視化、標準ポリシー整備から体制構築・訓練まで一貫支援します。さらに人材育成や情報共有、各国規制対応もカバーし、コンプライアンスと持続的成長を支える強固な体制を実現します。

09 セキュリティコンシェルジュサービス SERVICE

専任のセキュリティコンシェルジュが“いつでも相談できる身近な専門家”として伴走。対策検討や運用課題、最新脅威や法規制情報、ベンダー選定、インシデント対応まで状況に応じて柔軟に支援します。定期ミーティングやオンライン相談、レポートを通じて経営層と現場をつなぎ、中長期的な体制強化とリスク低減を実現します。

シンクタンクコンサルティング

当社ではこれまで、防衛セクターをお客様とする各種システム構築・換装等に係るプロジェクトの技術支援（Systems Engineering and Technical Assistance, SETA）分野で多くの実績・専門的知見を有しています。SETAにおける開発支援、業務遂行管理支援に加え、防衛・宇宙・サイバー分野に知見のある専門メンバーらにより、社内外ステークホルダーとも密に連携しお客様へ高い付加価値をご提供いたします。

01 シンクタンク・システムズエンジニアリングメニュー SERVICE

防衛・宇宙・サイバー分野等における国内外関連技術／政策／市場動向に関する調査分析

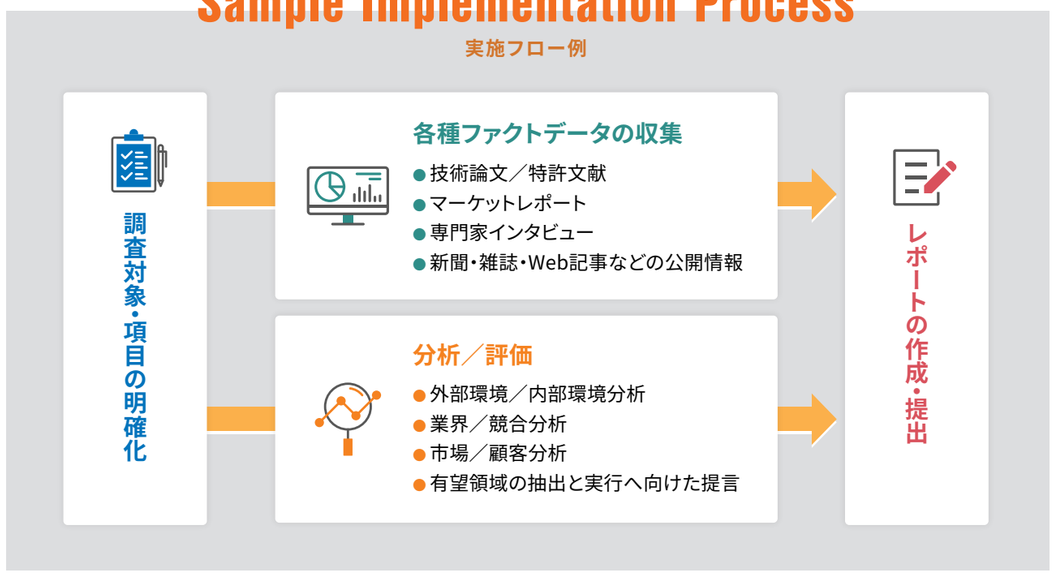
防衛・宇宙・サイバー分野の知見を活かし、新規事業や研究開発テーマ設定、政策検討に向けた実効性の高い調査・分析を提供。自組織では対応しきれない課題を補完し、テーマ設定や事業創出の実現性を高めます。

調査対象テーマ例

- 海外における関連技術／政策／市場トレンド分析
- 新規事業／研究開発ドメイン探索
- 官民連携などへ向けたスキーム構築支援

Sample Implementation Process

実施フロー例



02 プロジェクトマネジメントに係る技術支援（SETA） SERVICE

技術支援業務（通称SETA）を通じ、各種システム開発をはじめお客様の政策立案・研究開発計画策定等、プロジェクトマネジメント全般に係る適正な意思決定を支援いたします。

防御の視点を変えた、従来と全く異なる核心的な検知防御方法

Systems Engineering and Technical Assistance

お客様	SETA（MBSD）による提供価値
予算要求／見積	システム概念設計、市場・技術動向調査などを通じ、予算要求の精度・実現可能性を向上
要件定義作成	システム要件・見積のチェックや新たなニーズ発掘により、最良な要件定義を支援するとともに、潜在的な過剰コストを抑制
調達／契約	
設計／構築	システムの作りこみ・品質を第三者的視点からチェックすることでリリース後のシステム改修・障害対処コストを抑制
運用	システム改修要求のチェック、システム障害／不具合経験などを次期仕様にフィードバックすることでシステム利用者の満足度を向上

関連実績

- 中央官庁 IT投資計画策定支援コンサルティング
- 中央官庁 情報システムの設計・調達支援コンサルティング
- 中央官庁 宇宙機システム技術分野の教育
- 中央官庁 設備・機器等調達適正化に関する調査研究
- 中央官庁 宇宙政策に関する調査
- 研究機関 民生品の宇宙仕様化に関する調査検討