〇〇　御中

情報セキュリティ運用支援サービス

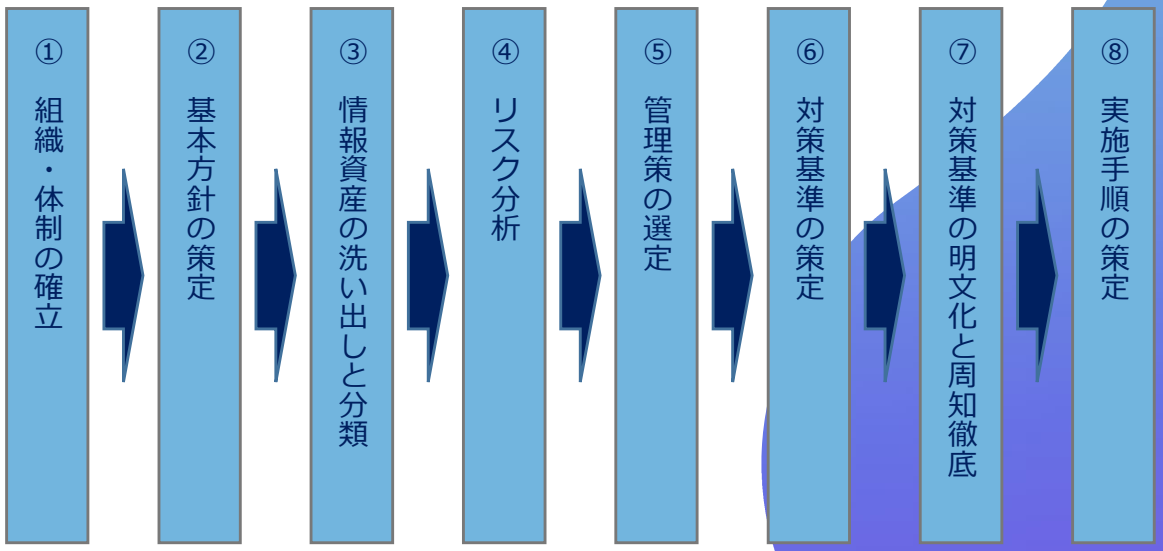
規程整備から、継続できる運用の立上げまで

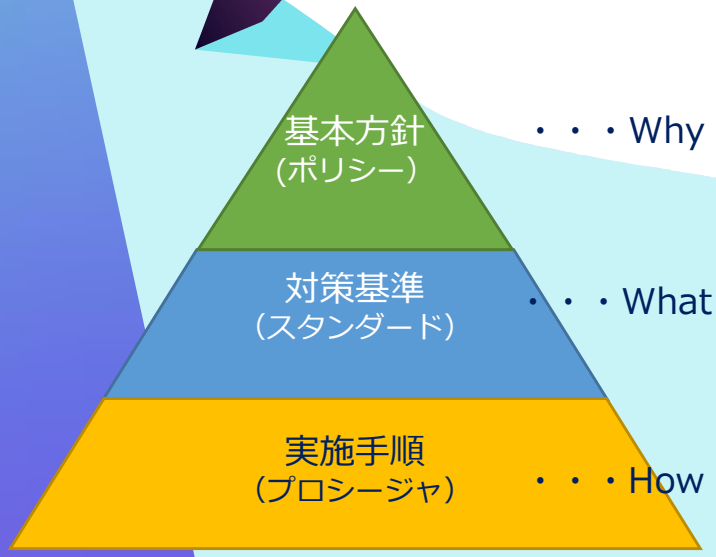
『人』と『デジタル』を絆ぐ

bitGate

情報セキュリティ対策は
～事業と取引関係に応じた段階的な取組み～

情報セキュリティでは、『機密性』、『完全性』、『可用性』に対する様々な脅威から守るべき情報資産を守ることが基本です。
そのために、『人的』、『物理的』、『技術的』、『組織的』な面から様々な対策を講じますが、当然、対策を行えば行うほどリソース（人、金、物）が必要です。



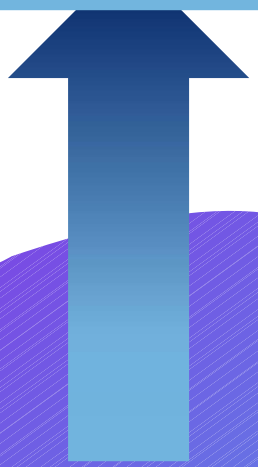


これらを現実的に対処するために体系的かつ系統立ててとらえたのが情報セキュリティマネジメントシステム（ISMS:Information Security Management System）ですが、
ISO27001はゴールではなく、中小企業は「まず説明できる状態」が重要です。

終わりなきセキュリティ対策

情報セキュリティは運用にコストとリソースが必要。でも売上に直結しない投資であるため、多くの中小企業は認証を取得するレベルまでの対策をしない…

対応度を上げるとコストも上がる



ISO27001(ISMS)認証取得

認証取得に数百万の費用と半年程度の期間が必要。大企業の多くが導入。グローバル取引には海外の認証取得も必要となる。

IPAセキュリティ対策実施

中大手企業が独自の情報セキュリティポリシー策定に利用している。ガイドや情報素材は無償だが独自でPDCAを回す必要。

セキュリティ対策設備導入のみ

中小企業の多くがシステム導入によるセキュリティ対策担保までとなっている。ルールは明文化されず個人まかせとなっている。

現状

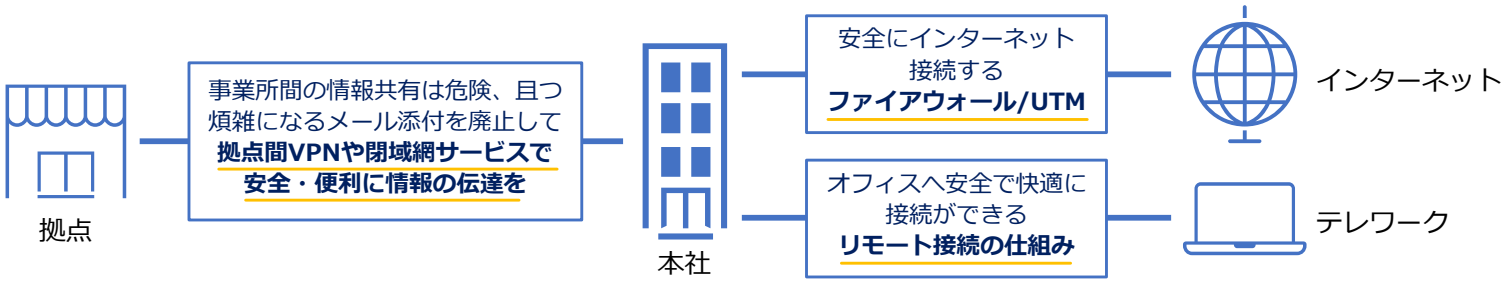
中小企業向けにIPAをはじめとするガイドはリリースされているが、専門知識が無いため具体的に何をすれば良いのか分からず、ITベンダーから紹介されたシステムの導入だけで済ませている企業が多い。

本サービスでは、 ISO27001の考え方を参考に整理されたIPA推奨の情報セキュリティガイドラインのテンプレートと、経産省が整理している「要求事項・評価基準案」を組み合わせ、★3または★4相当のどこを目指すかを整理したうえで御社の情報セキュリティガイドラインを整備します。

技術対策は「ルールと運用」があって初めて機能します

新型コロナウイルスをきっかけに、テレワークを導入した企業も多いかと思います。しかし、安易なリモートアクセス環境で運用すると、インターネットのサイバー脅威にさらされ、PCが乗っ取られたり情報漏えいするなどの事業継続に影響する事態に陥る可能性が高まります。

安全で便利なテレワーク環境に必要な設備



個人所有などの外付けメディアを利用させない**デバイス制御**

サイバー脅威から守る**エンドポイントセキュリティー対策**

情報漏えいの心配が少ない**PCのデータレス化**

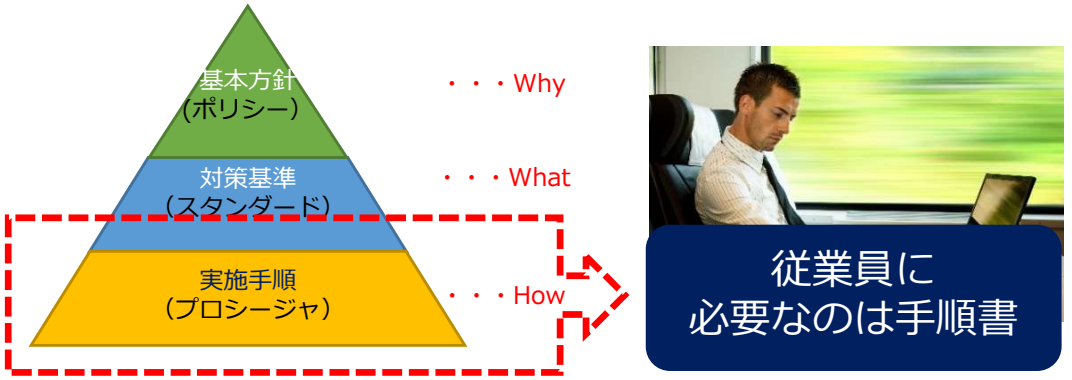
Check!

これらの設備を使うのは「社員」の皆さんですが、使い方やルールは徹底されていますか？

設備を整えてもルールが不明確では個人ごとの判断で事故が起きやすくなります。
きっかけは些細な情報漏えいでも、事業復帰までに多大なコストと時間を浪費し、
結果的に**企業の信用を失い事業継続にも影響**することが起きています。
本サービスは、特定の機器やシステム導入を目的とするものではなく、規程と運用を前提として、
必要に応じて技術対策を整理します。

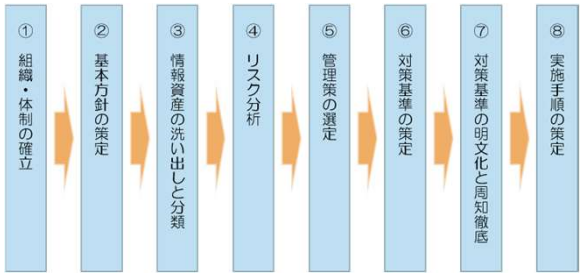
ベストプラクティスからはじめる情報セキュリティ対策

対策レベルに関わらず、ルールを遵守するのは従業員です。
従業員は与えられた設備を使って業務を遂行します。
業務遂行時の情報セキュリティ対策には明文化された手順が必要です。



手順書を作成するために、情報セキュリティ対策の標準プロセスでプロジェクト化するにはコストがかかるため、要求事項・標準基準をベースに標準プロセスの後半に実施する手順を照らし合わせて、取り組める範囲を決めることで、無理な運用を組み込こむことなくスタートすることが可能です。

【正方向】
ハードルが高い



【逆方向】
要求事項・評価基準をベースに取り組めるものをチョイス

情報セキュリティ運用ガイド作成支援サービス

ISO27001認証取得までは考えていない

最低限の情報セキュリティのルールは作りたい

対策整備にあまりコストと時間をかけたく無い

上記のようなご要望をお持ちのお客様に最適です。

1. IPAセキュリティ診断実施（可視化）
2. IPAテンプレートをベースにした規程作成
3. 要求事項・評価基準案（経産省）による
   ギャップ整理★3相当から検討
4. 運用設計（教育・記録・説明の仕組み）取引
   先対応を見据えた整理

IPAセキュリティ診断

現状把握
（可視化）

ワーキング

（４～５回）

IT設備

IPA
テンプレート

次期対応
課題リスト

ITシステムの現状調査

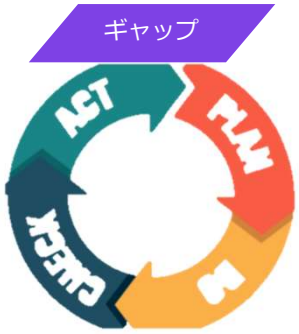
※オプション

全社展開

情報セキュリティ運用ガイド作成支援サービスの期待効果

ベースラインによる現状把握

ベースラインができることで、市場要求におけるリスクとのギャップが把握可能となります。ギャップが明確になるとリスク対策が立案できるので、是正や強化など継続活動のPDCAが回りやすくなります。



業務の可視化と改善

セキュリティ対策強化における、利便性とのトレードオフでは業務プロセスの可視化が必要になることがあります。業務プロセスの可視化とセキュリティのリスクヘッジを合わせて検討することで、俗人化や工数肥大などの洗い出しができ、合理化、省力化など業務改善を期待できます。

リテラシー向上とCSR活動

情報セキュリティ対策が『お客様や取引先との関係に重要である』こととして理解を深めさせるために、ガイドラインを入社時などの社員教育用資料として活用。従業員のリテラシーが向上することで、高品質な顧客対応を目指しCSR（またはSDGｓ）へ導きます。

支援サービス活動の基本的な進め方

お客様

- 必要知識の吸収
- 検討事項、実行事項の確認
- 前回以降実施事項の結果報告

弊社

- 必要知識・検討ポイントの提示
- 活動進捗確認
- 宿題の提示

1～2 h

ワーキング

- 検討事項の協議
- 宿題事項の提出
- 実行事項の実施

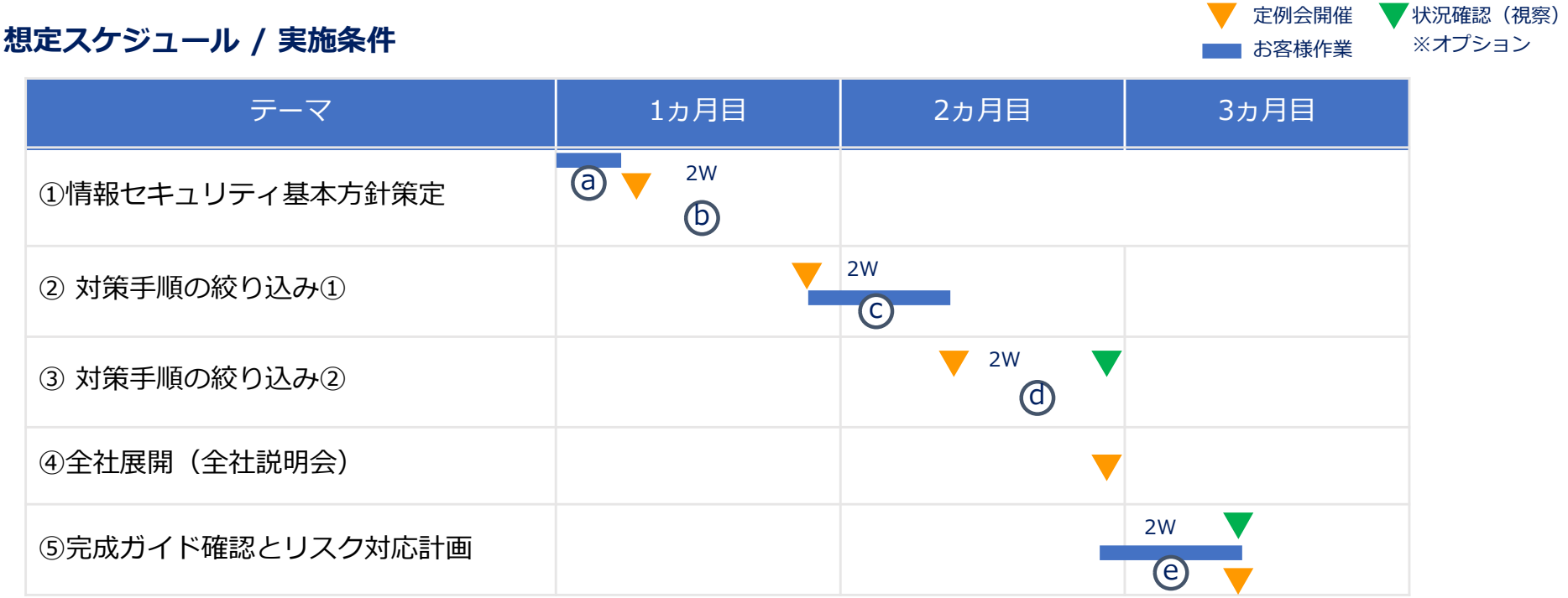
- 次のＷＧの準備
- 提出いただいた宿題のチェック

この期間
約1～3週間

次の定例会

ワーキングスケジュール（例）

- **想定スケジュール / 実施条件**



- **対象範囲**
  - 1拠点での開催
  - お客様事務局メンバーとの協議
- **期間/回数/時間**
  - 約3カ月間 / ワーキング4回＋全社展開支援1回 （max2h/回）
- **サービス実施方法**
  - 事務局様への講義・ディスカッション方式です。
  - 弊社は定例会の中で基礎情報や事例などノウハウをお話し、次のワーキングまでにお客様にて宿題事項を実施していただく流れで進めます。
  - 講義資料・成果物サンプル・帳票などをツールとしてご提供いたします。弊社の提示した考え方に基づき、お客様が自社の状況に合わせてカストマイズや最終化をお願いいたします。

ワーキング概要

テーマ	定例会概要	お客様の実施事項	成果物
受注直後又は受注直前	**プロジェクト進行確認会** ➢事務局担当者と進行に関するすり合わせ 10：00～11：00（1時間）	a ●事務局メンバー選定 ●各部セキュリティ診断 ●門リーダーの選定 ●IPA情報資産台帳ドラフト版作成	IPAセキュリティ診断結果 情報資産台帳ドラフト版
プロジェクトキックオフと基本方針決定	**ワーキング ①** ➢プロジェクトメンバーとの目的/計画の共有 ➢現状の共有（診断結果） ➢情報セキュリティ基本方針策定 10：00～12：00（2時間）	b ●宿題項目の準備	
対策手順の絞り込み①	**ワーキング ②** ➢情報セキュリティ規程策定 10：00～12：00（2時間）	c ●宿題項目準備	
対策手順の絞り込み②	**ワーキング ③** ➢情報セキュリティ規程策定（残り） ➢初版情報セキュリティハンドブック確定 ➢全社展開内容協議と準備 10：00～12：00（2時間）	d ●宿題項目準備 ●社内展開準備	情報セキュリティハンドブック
全社展開	**全社展開支援** ➢説明会開催または説明会開催支援 10：00～12：00（2時間）	e ●宿題項目準備	
ガイド完成	**ワーキング ④** ➢ガイドブックチューニング※必要に応じ ➢維持管理活動手順策定 ➢初版情報セキュリティ運用ガイド確認 ➢情報セキュリティリスク対応計画暫定版確認 10：00～12：00（2時間）		情報セキュリティガイド 情報セキュリティリスク対応計画

期間：2～3ヶ月
金額：80万円/月～
※期間、金額とも内容によって変動します

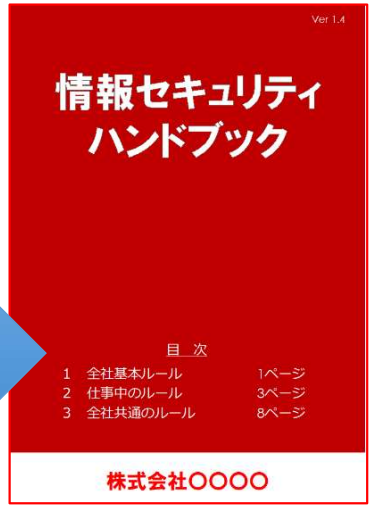
成果物見本

標準サービス

推進メンバー用

第1章　情報セキュリティ基本方針
第2章　情報セキュリティ対策基準
　　2.1　組織的対策
　　2.2　人的対策
　　・・・
第3章　情報セキュリティ対策手順
　　3.1　基本ルール
　　3.2　電子メールの利用
　　3.3　インターネットの利用
　　・・・
第4章　維持管理活動
　　4.1維持管理活動
　　・・・

抜粋



従業員配布用

その他付帯資料サンプル
・授受管理表、誓約書など

オプションサービス

現状調査

情報資産管理台帳作成

情報ポータル作成
SharePoint等