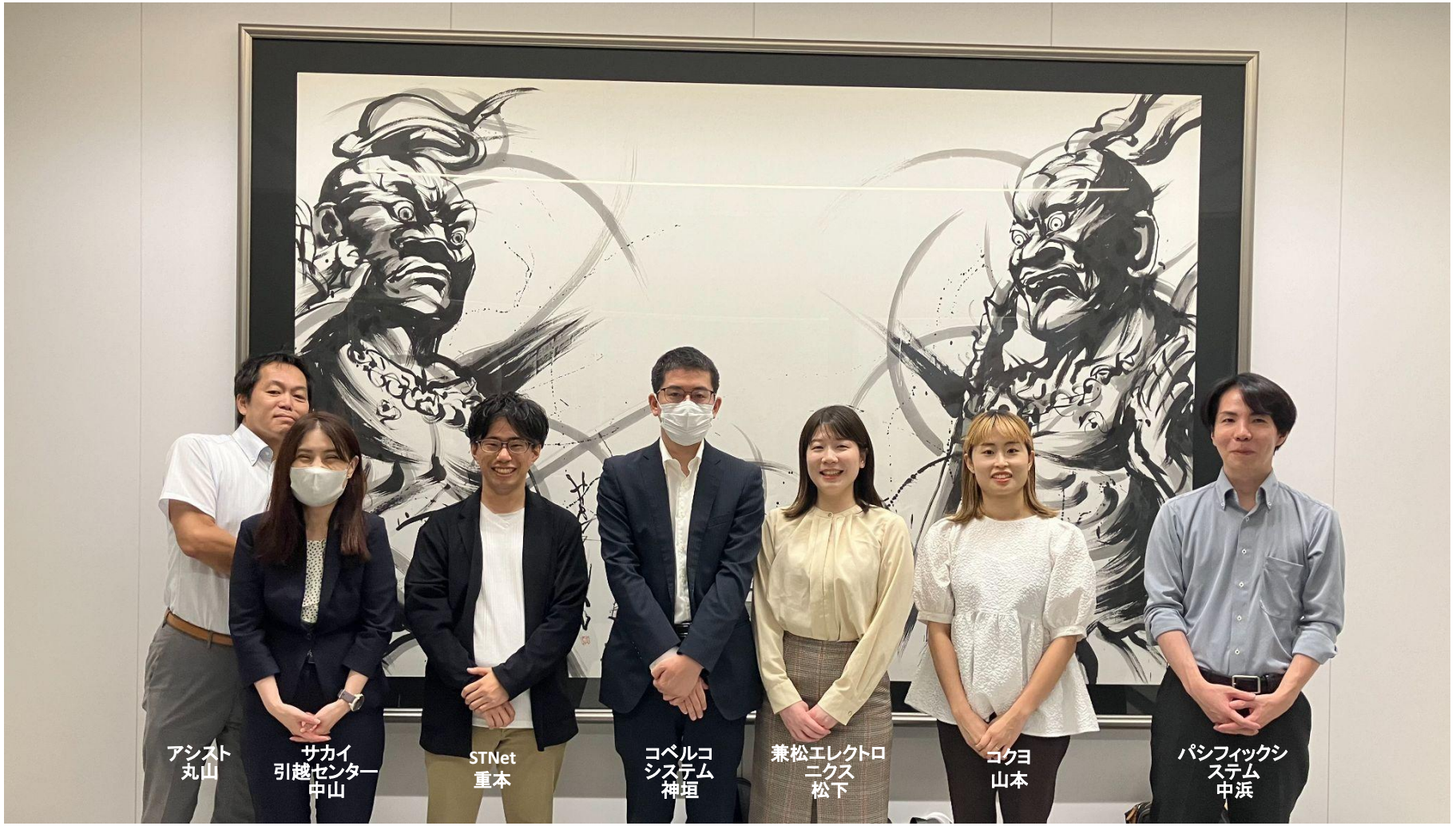
サイバー攻撃手法の分析と企業対策分科会

情報の海で迷わないために ～サイバーセキュリティの取捨選択～

サイバー攻撃手法の分析と企業対策分科会メンバー紹介



サワイ
グループHD
橋本

アシスト
高橋

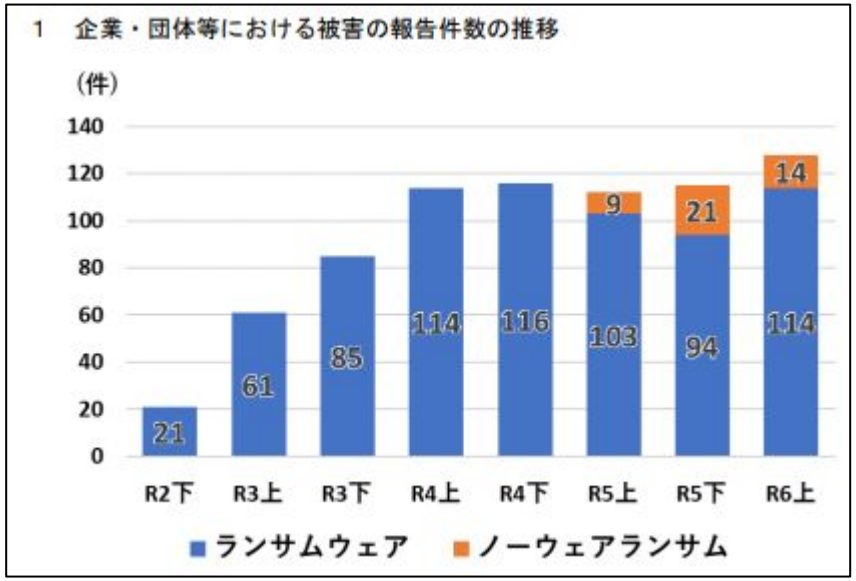
ひろぎんITソ
リューションズ
金木

STNet様 データセンター Powerico(パワリコ)見学時撮影

研究の背景

- 令和6年度 情報通信白書のサイバー攻撃に対する通信数の増加や、警察庁のランサムウェア被害の統計より、サイバー被害は年々増加している

NICTERにおけるサイバー攻撃関連の通信数の推移



ランサムウェアの被害に関する統計より、企業・団体等における被害の報告件数の推移

セキュリティ関連情報は巷にあふれている

世の中にはたくさん参考資料はあるけれど…

↓参考資料

- 情報セキュリティ10大脅威
- 安全なウェブサイトの作り方
- 情報セキュリティ白書
- JPCERT/CCのレポート
- OWASP Top 10
- NIST サイバーセキュリティフレームワーク

資料がたくさんあってどれを参考にすれば良いか？

見ている資料は最新版なのか？

書いてある内容を理解するには勉強しないと難しい…

一方、企業におけるセキュリティ対策の現状は？

採用しようにも、いま
セキュリティ人材の
数が少なくて。。。

セキュリティ？
ウチでは見えない
ところにそんなにコ
ストはかけられな
いよ。。

企業によって対策状況に大きな差がついているのでは？

→　セキュリティ対策チェックシートで、各企業の状況を確認してみる

セキュリティ対策チェックシートについて

- 1.　評価の実施

10の指標について、自社の対応状況をスコア（例: 1～5段階）で評価する

1.サイバーセキュリティリスクの認識	6.PDCAサイクルを活用した継続的な改善
2.サイバーセキュリティ管理体制の構築	7.インシデント発生時の緊急対応体制の整備
3.対策のための資源（予算・人材等）の確保	8.事業継続・復旧体制の整備
4.サイバーセキュリティリスクの把握と計画策定	9.サプライチェーン全体の状況把握と対策
5.リスクに対応する仕組みの構築	10.情報の共有・開示と連携促進

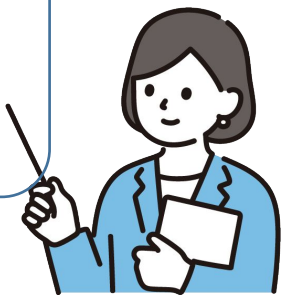
- 2.　課題の抽出

評価結果を基に、特にスコアが低い項目を特定し、優先的に改善すべき課題を明確化する

- 3.　改善計画の策定

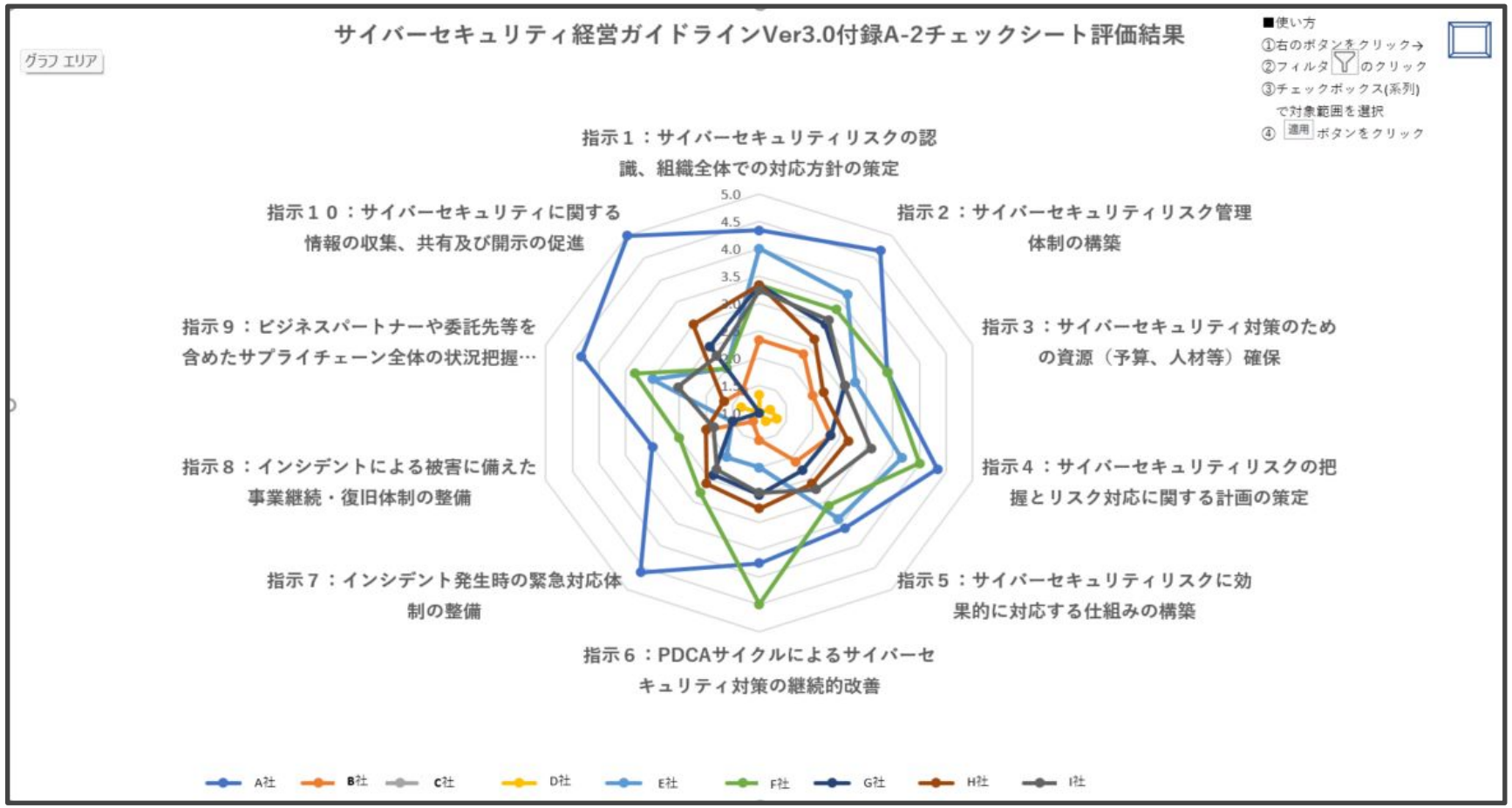
課題に基づいて具体的なアクションプランを立案し、サイバーセキュリティ体制を強化する

自社に足りないものがわかり、次に何をすべきか分析できます



参加メンバーでチェックシートから状況確認！

↓参加メンバー各社の評価集計結果



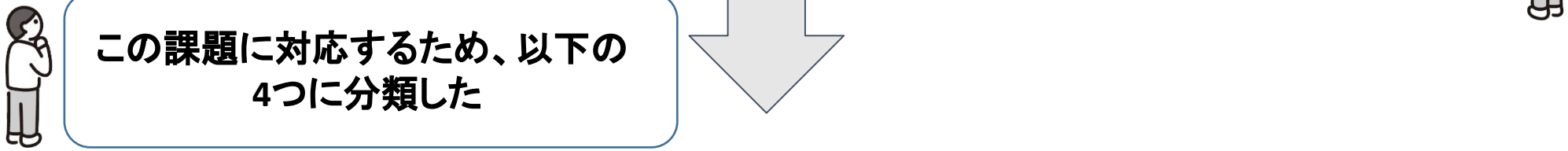
共通して弱いところがある…

企業ごとに差がある…

チェックシートの評価結果より出てきた セキュリティ対策の課題

インシデント発生時の緊急対応体制の整備

インシデントによる被害に備えた事業継続・復旧体制の整備



1. ビジネス継続計画（BCP）
2. 事前対策（防御）
3. インシデント発生時の対応策
4. セキュリティ教育

研究を進める中での課題

各社共通のウイークポイントから、
対応策を4つに分類分けすることはできたが…

1. ビジネス継続計画（BCP）	3. インシデント発生時の対応策
2. 事前対策（防御）	4. セキュリティ教育

各社ごとに環境や優先順位が異なるため

すべての企業に当てはまる具体策を提言するのが難しい！！

そこで…

架空のP社を立てて 現実的なセキュリティ対策の進め方の 方法論を作成する！
※経営層へ中長期計画の提案

架空の企業P社についての会社概要

主要な 事業内容	運送と運送に伴う 付帯サービス業務
会社名	株式会社P
年商	単体：800億円規模 グループ全体：900億
従業員	単体：5000名規模 グループ全体：6000名規模

P社の業務内容について

本社

事務職

営業所

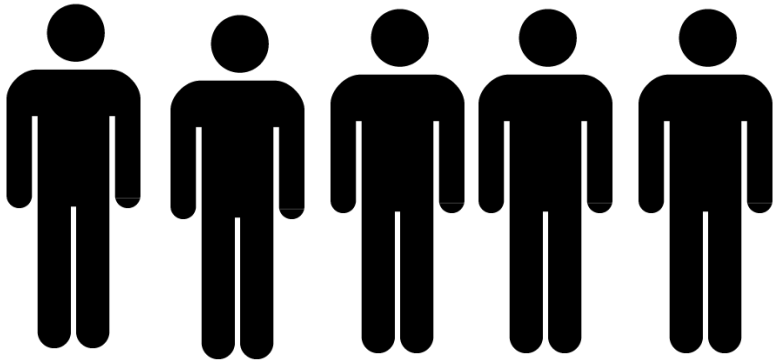
営業員

現場職

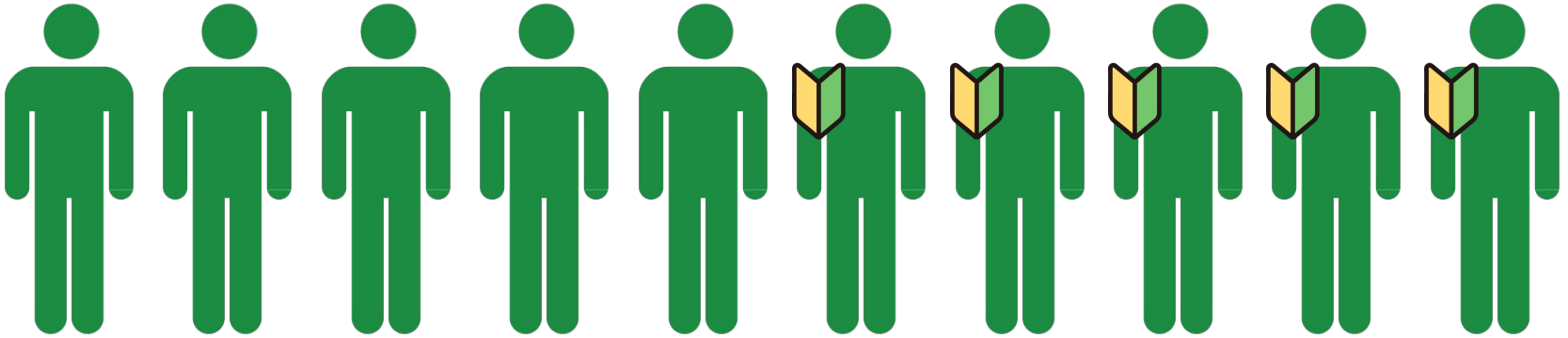
グループ会社

現場職

情報システム部設定について

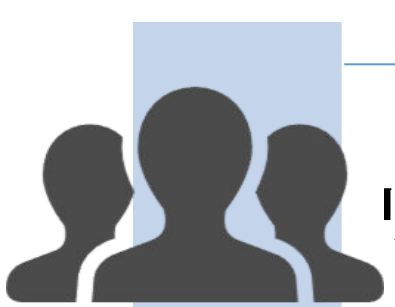


勤続歴10年以上

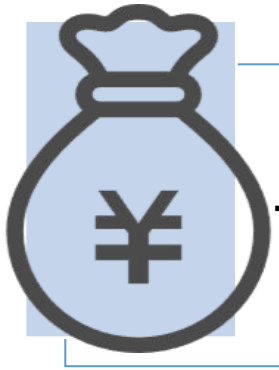


世代交代における
ノウハウの継承に
課題感がある

P社のセキュリティ対策の課題



リソース不足



予算制約

セキュリティ教育の不足

インシデント対応の遅れ

クラウドセキュリティの課題

リソース不足

過剰な業務負荷

専門知識不足

業務の属人化

セキュリティ教育の不足

フィッシング攻撃への脆弱性

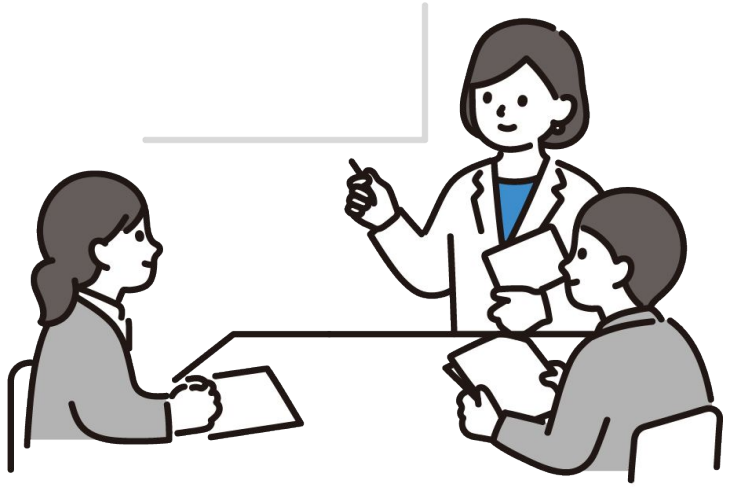
パスワード管理の不備

ソーシャルエンジニアリングへの対策不足

予算制約

セキュリティツールの導入不足

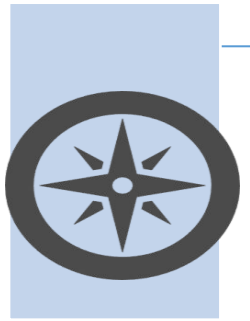
人材の確保が困難



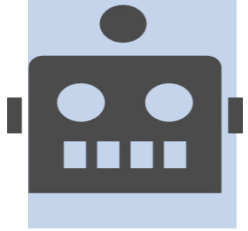
継続的なセキュリティ教育の欠如

今後P社に求められる姿

現状分析とリスク評価



セキュリティポリシーとガバナンス



技術的対策の実装

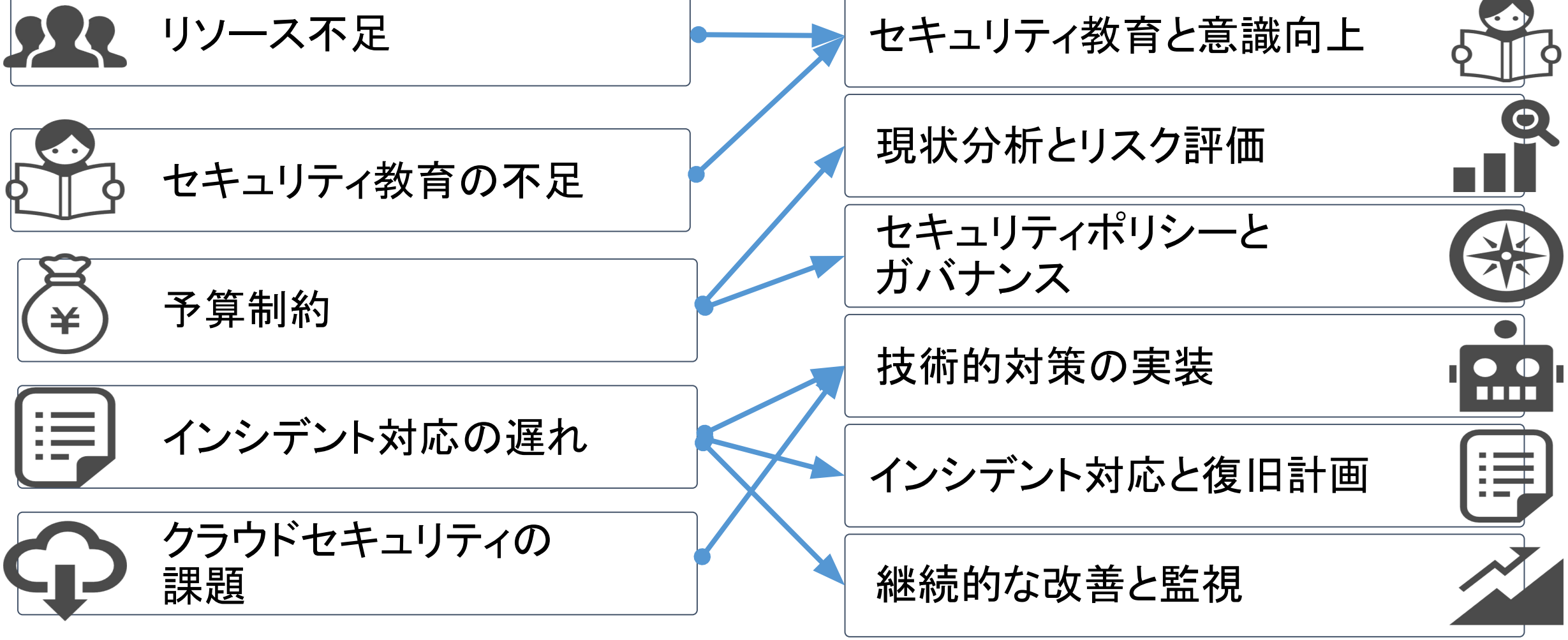
インシデント対応と復旧計画

セキュリティ教育と意識向上

継続的な改善と監視

P社の課題と対応策

課題	対応策
リソース不足	セキュリティ教育と意識向上
セキュリティ教育の不足	現状分析とリスク評価
予算制約	セキュリティポリシーとガバナンス
インシデント対応の遅れ	技術的対策の実装
クラウドセキュリティの課題	インシデント対応と復旧計画
	継続的な改善と監視

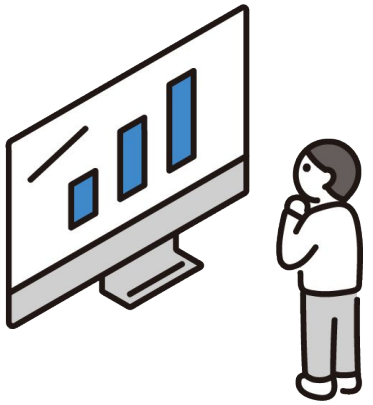


現状分析とリスク評価

既存のセキュリティ対策の評価

脆弱性の特定

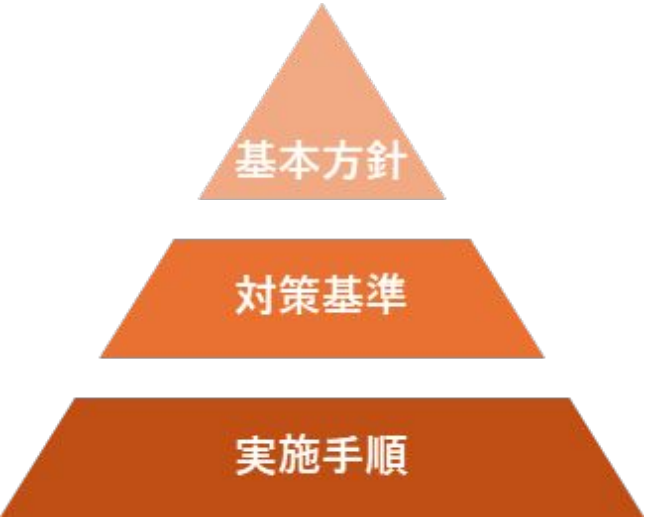
潜在的な脅威の分析



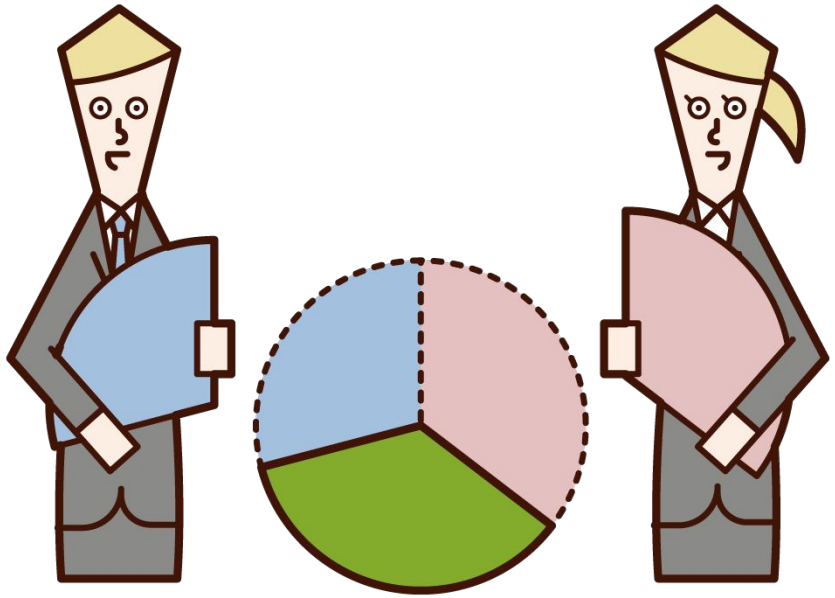
分析結果をわかりやすく上層部にレポートすることで現状のセキュリティに対する危機感を持ってもらい、スムーズな予算の確保につなげる

セキュリティポリシーとガバナンス

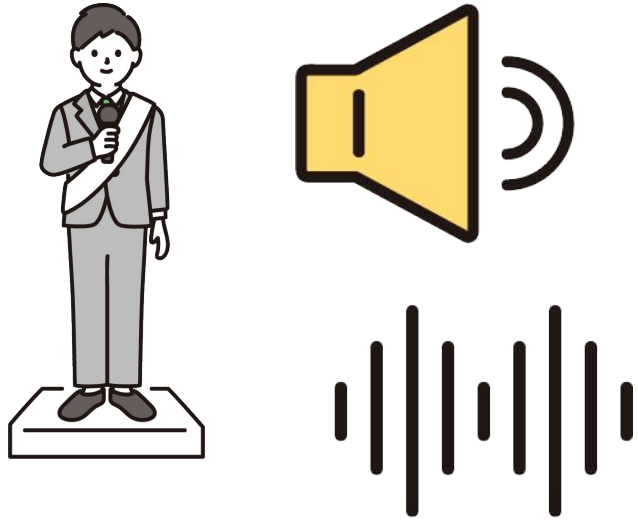
セキュリティ
ポリシーの策定



役割と責任の明確化



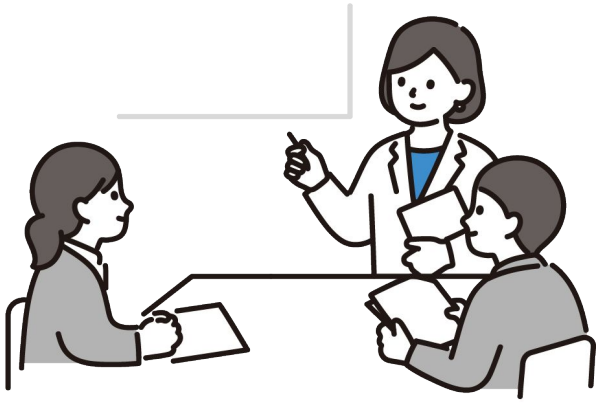
セキュリティ
ガバナンスの強化



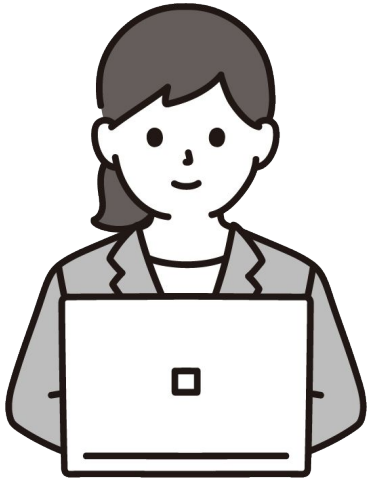
ポリシーやガバナンス策定において適切に経営層を巻き込んでいくことで
セキュリティに対する理解を深めてもらう

セキュリティ教育と意識向上

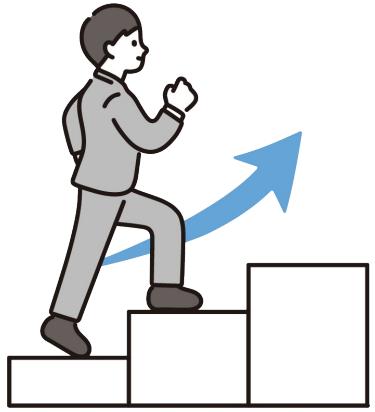
定期的な
セキュリティ教育



実践的な訓練



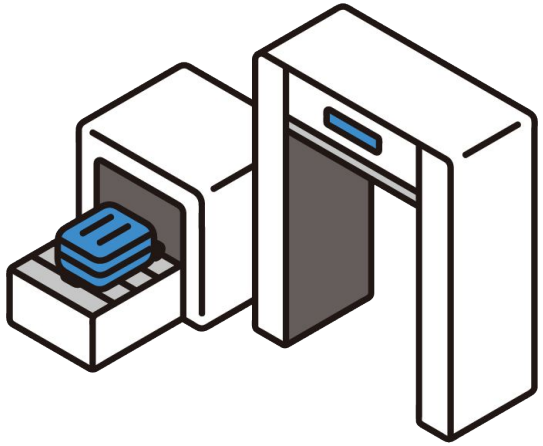
社員のスキルアップ



会社全体でサイバーセキュリティへの意識向上を図ることで、情報システム部の取組への理解を深め、将来的なセキュリティ人材の確保に繋げる

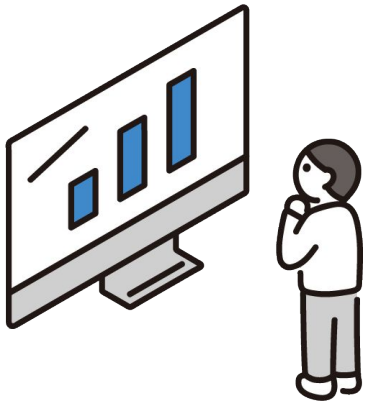
継続的な改善と監視

定期的な脆弱性スキャン



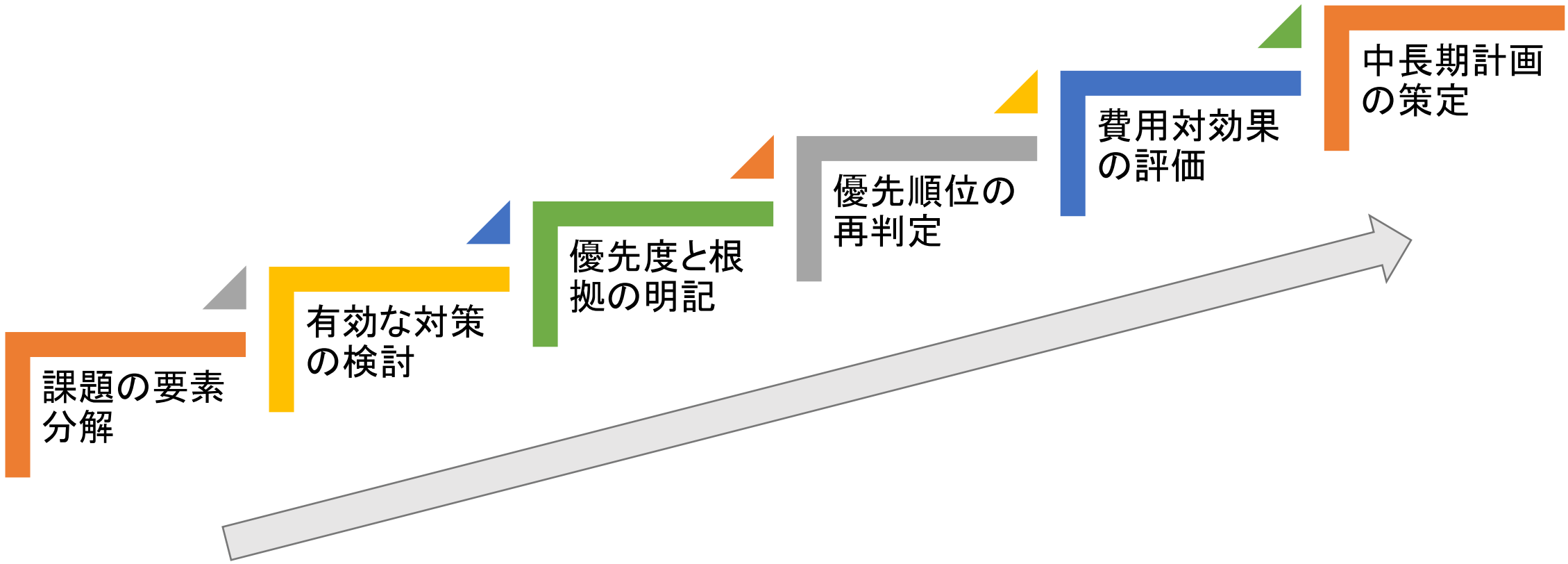
セキュリティパッチの適用

セキュリティインシデントの報告と分析



インシデント発生時に迅速に対応を開始することが可能となり、サイバーインシデントによる被害を最小化することが可能となる

P社のセキュリティ対策のロードマップ



P社セキュリティ中長期計画策定に向けて

1. ビジネス継続計画（BCP）
2. 事前対策（防御）
3. インシデント発生時の対応策
4. セキュリティ教育

P社の課題に対する取り組み項目を洗い出し

Endpoint Detection and Response（EDR）	サプライチェーン対策	導入済み機器を活用した セキュリティ対策の強化	情報資産棚卸
多要素認証	Mobile Device Management （MDM）	システムの可視化と外部媒体 利用制限	脆弱性管理
セキュリティ教育 （新任者向け）	セキュリティ啓蒙教育 （新技術、攻撃に対して）	情報システム部門人材育成	BCP策定 (業務システム洗い出し）
BCP策定（システムを用いない 業務運営）	緊急時対応体制の構築	BCP策定 （机上での復旧対応演習）	サイバーセキュリティ保険加入

P社セキュリティ中長期計画

2025年～2030年の期間で
取り組み項目に優先順位を
付け、スケジュール化

区分	項目	優先順位	2025年度				2026年度				2027年度				2028年度				2029年度				2030年度			
			1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
事前対策（防御）	Endpoint Detection and Response（EDR）	中						■																		
事前対策（防御）	サプライチェーン対策	低							■																	
事前対策（防御）	導入済み機器を活用したセキュリティ対策強化	高	■				■				■				■				■							
事前対策（防御）	情報資産棚卸	高		■				■				■				■				■						
事前対策（防御）	多要素認証	低						■																		
事前対策（防御）	Mobile Device Management（MDM）	中							■																	
事前対策（防御）	システムの可視化と外部媒体利用制限	中	■																							
事前対策（防御）	脆弱性管理	低											■													
セキュリティ教育	セキュリティ教育（新任者向け）	高	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
セキュリティ教育	セキュリティ啓蒙教育（新たな攻撃や被害に対する）	中	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
セキュリティ教育	情報システム部門人材育成	低				■				■				■				■				■				■
ビジネス継続計画（BCP）	BCP策定（業務システム洗い出し）	中			■																					
ビジネス継続計画（BCP）	BCP策定（システムを用いない業務運営）	中					■	■																		
インシデント発生時の対応策	緊急時対応体制の構築	中							■	■																
インシデント発生時の対応策	BCP策定（机上での復旧対応演習）	中										■				■				■						
インシデント発生時の対応策	サイバーセキュリティ保険加入	低											■													

■優先度
高：最優先で対応する
中：高の対応を踏まえて
　　対応を進める
低：中の対応を踏まえて
　　対応を進める

中長期計画における
P社がやるべきセキュリティ対策

項番	対策	優先度
A	**情報資産棚卸**	高
B	**セキュリティ教育（新任者向け）**	高
C	**導入済み機器を活用したセキュリティ対策強化**	高
D	システムの可視化と外部媒体利用制限	中
E	BCP策定（業務システム洗い出し）	中
F	緊急時対応体制の構築	中
G	セキュリティ啓蒙教育（新たな攻撃や被害に対する）	中
H	BCP策定（システムを用いない業務運営）	中
I	BCP策定（机上での復旧対応演習）	中
J	Endpoint Detection and Response（EDR）	中
K	Mobile Device Management（MDM）	中
L	脆弱性管理	低
M	サプライチェーン対策	低
N	サイバーセキュリティ保険加入	低
O	情報システム部門人材育成	低
P	多要素認証	低

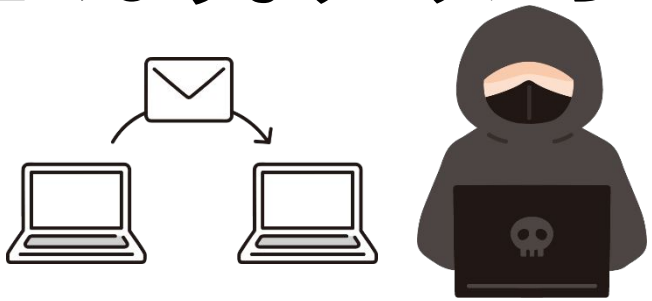
対策A:情報資産棚卸

- 情報資産が整理されていないと…?

どのような被害を

どうやって防げばいいか

どのようなリスクから



対策A:情報資産棚卸

- 会社を被害から守るために情報資産の棚卸が必要

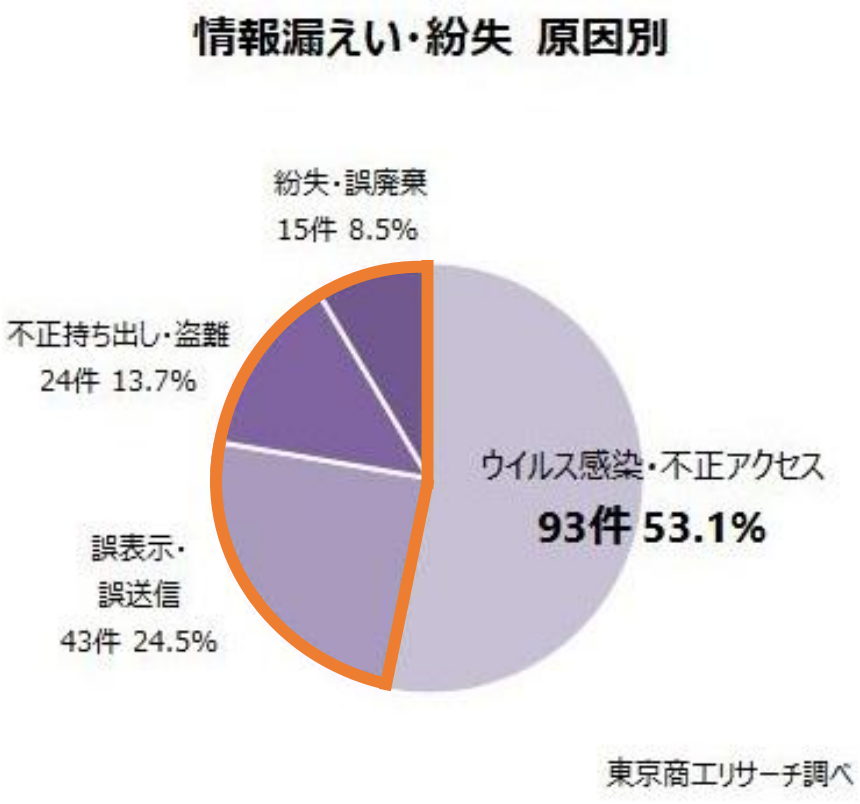
情報資産管理台帳

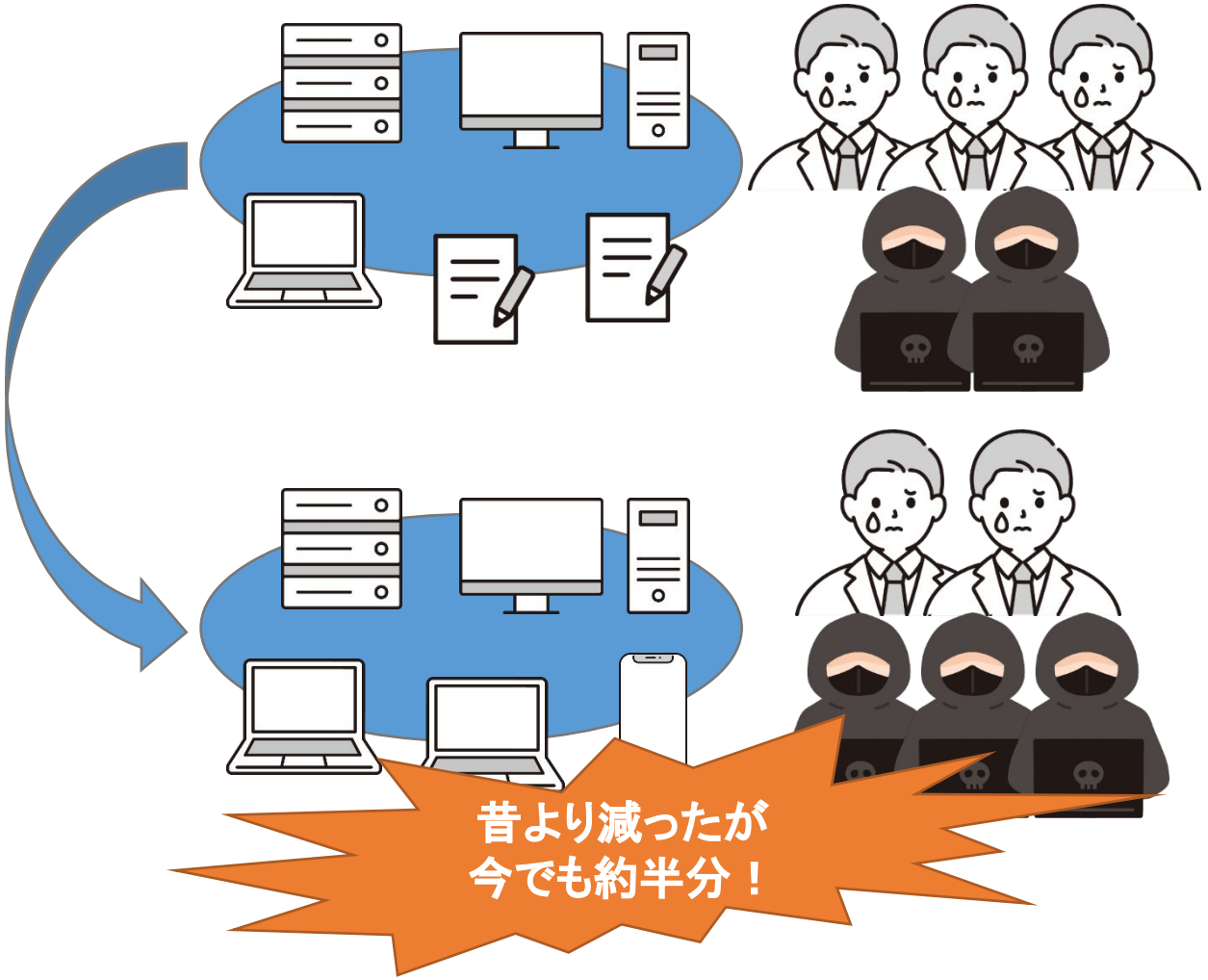
業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）					
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	**3**		#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	**3**		#####	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	**3**	5年	#####	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	**3**	7年	#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				2	2	2	**2**		#####	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				2	2	2	**2**		#####	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3	**3**		#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			3	3	3	**3**		#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	社内サーバー	有			3	3	3	**3**		#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			3	2	2	**3**		#####	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	モバイル機器	有			3	2	2	**3**		#####	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大

出典: IPA リスク分析シート

対策B:セキュリティ教育（新任者向け）

- セキュリティ事故に占める人的要因の割合は **約47%**



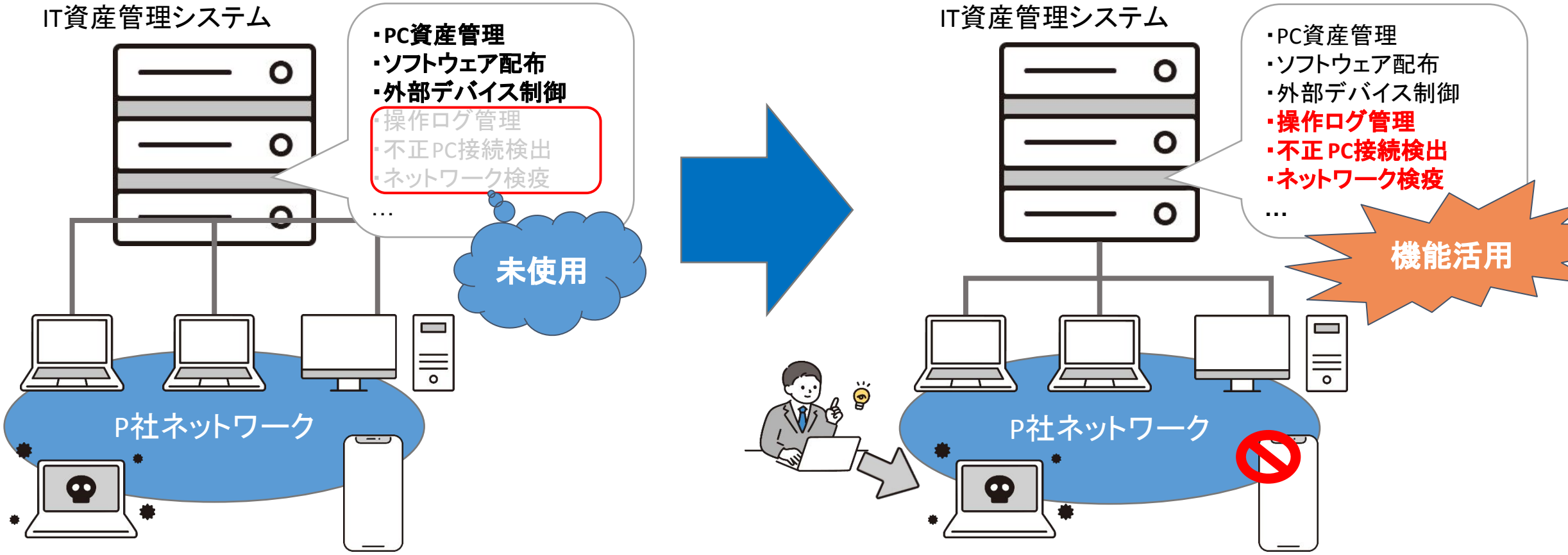


対策B:セキュリティ教育（新任者向け）

- 社員一人一人が適切な情報セキュリティの知識を身に着ける必要がある
- 特に新任者はセキュリティ知識がない可能性があり重点的な教育を実施するべき

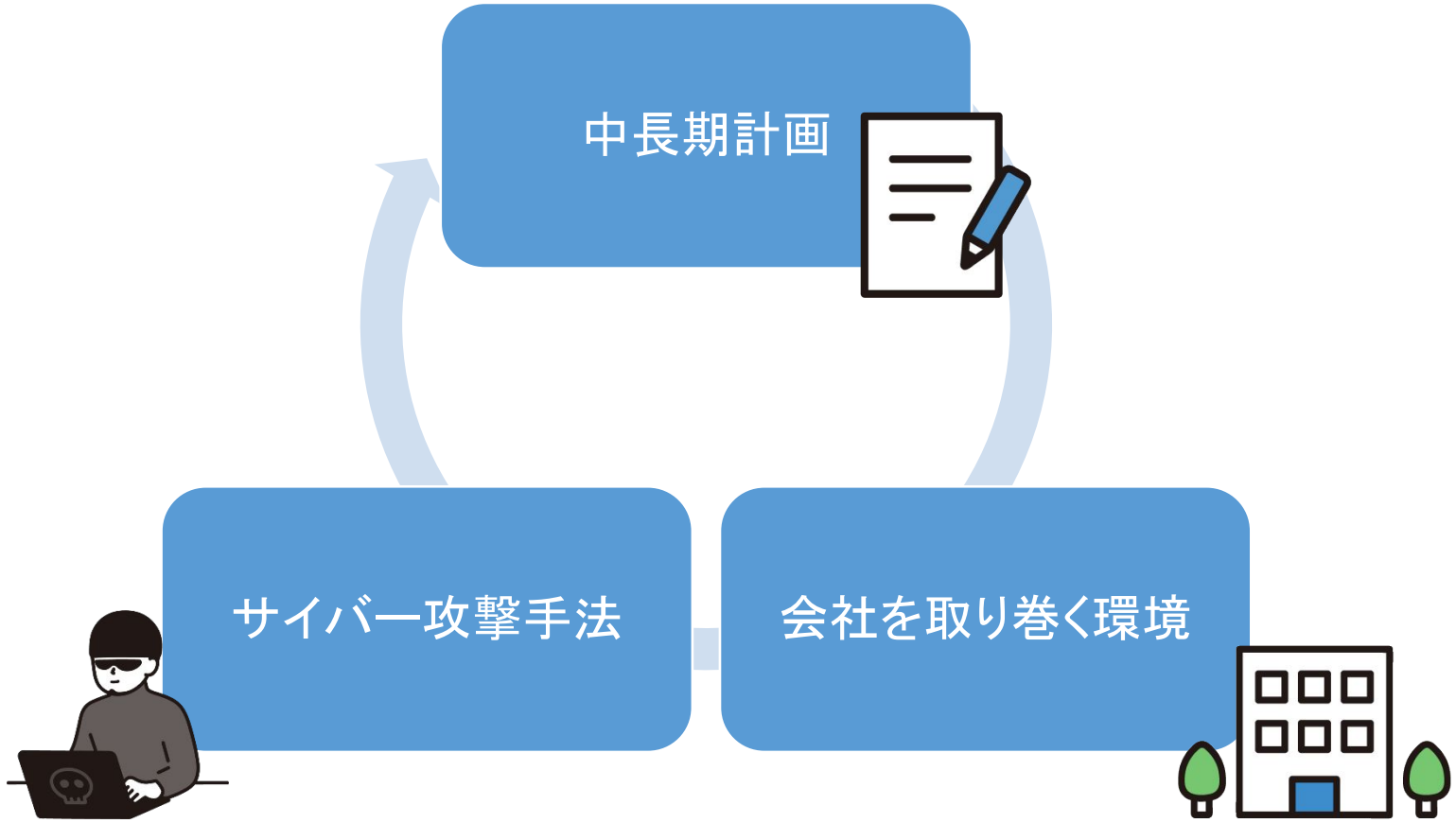
対策C:導入済み機器の活用

- 導入済み機器の有効活用でローコストでセキュリティ強化も可能な場合もある



サイバーセキュリティ中長期計画の有効性検証法

中長期計画は定期的に見直しが必要！



中長期計画 再評価のためのポイント

1. 実施したセキュリティ対策の評価
2. 外部環境の変化を計画に反映

1 実施したセキュリティ対策の評価

Ⅰ．セキュリティ対策の有効性を評価する

・チェックシートを作成し評価 ※投資額、効果、攻撃された場合の損失など…

・IPAの「サイバーセキュリティ経営可視化ツール」を定期的に実施

Ⅱ．従業員のセキュリティ意識の変化を把握する

・セキュリティに関するアンケート実施

・従業員起因で発生したセキュリティインシデント件数の集計・比較

2 外部環境の変化を計画に反映

Ⅰ. 新たな脅威や脆弱性情報の収集

・セキュリティ情報サイトを活用し、情報収集を行う

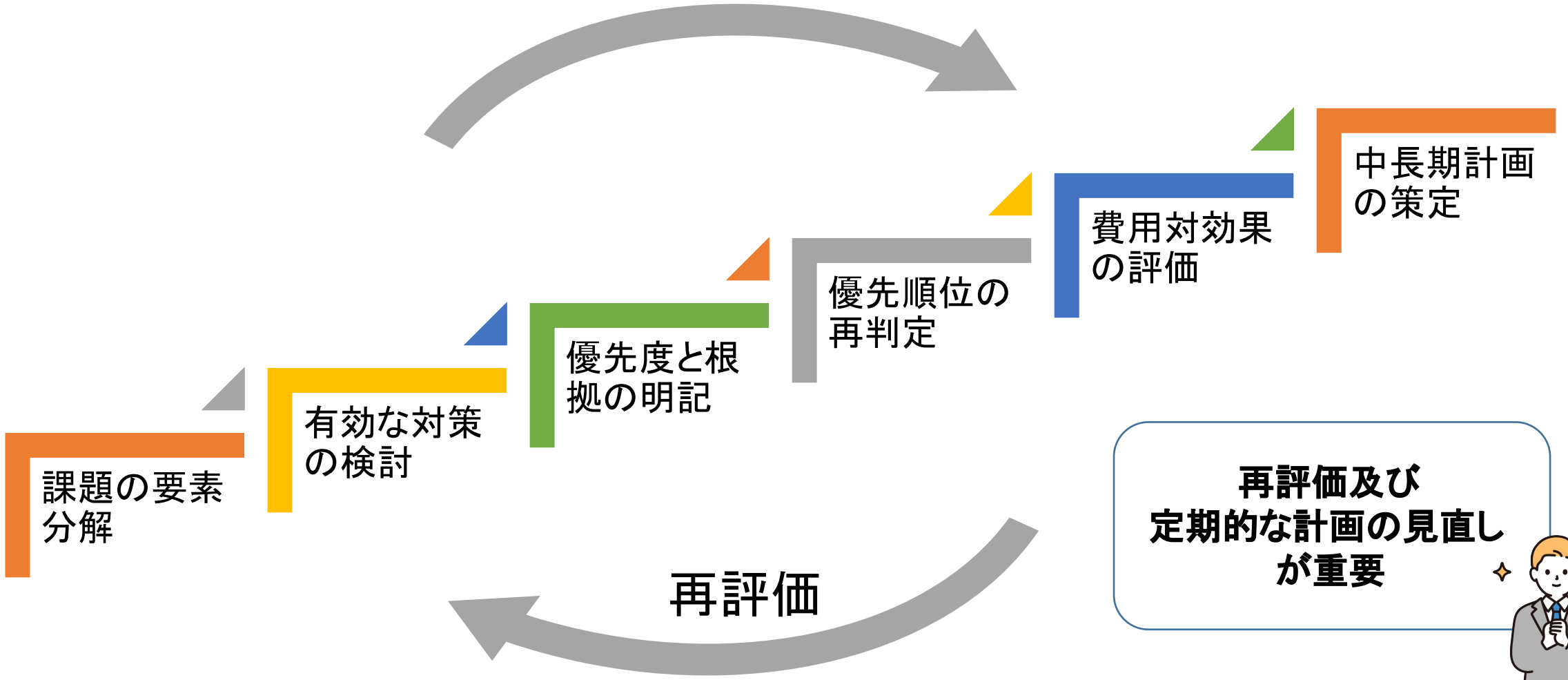
例：IPA (独立行政法人 情報処理推進機構) JPCERT/CC (日本CERT協議会) Security Nextなど…

Ⅱ. ビジネス環境の変化

・ITツールのトレンドや働き方などの変化に応じて、計画を変更する

例：クラウド利用の拡大、リモートワークの増加等

P社のセキュリティ対策のロードマップ（再評価）



再評価及び定期的な計画の見直しが重要

まとめ

近年増加するサイバー攻撃に対して、企業としてのセキュリティ対策を考える取り組みをテーマとして進め、下記内容を作成した

・架空のP社を例とし、セキュリティ課題と求められる姿に近づくための対策方法を検討

・P社が実現可能な期間、コスト、内容を踏まえ、対策方法を実現するための中長期化計画の　立案を実施。（今後、各社が活用するための一例として用意）

ただ、実際の活動結果の検証までは行えていないため、本資料を基として下記活動が今後必要と考える

・自社に合わせた中長期計画の策定から実行

・セキュリティ対策評価や、外部環境変化にあわせた、中長期計画の改善による数年置きで　の再評価

今後は作成したP社を作例として、
各社で取り組むセキュリティ対策の最初のステップとなれば良いと考える