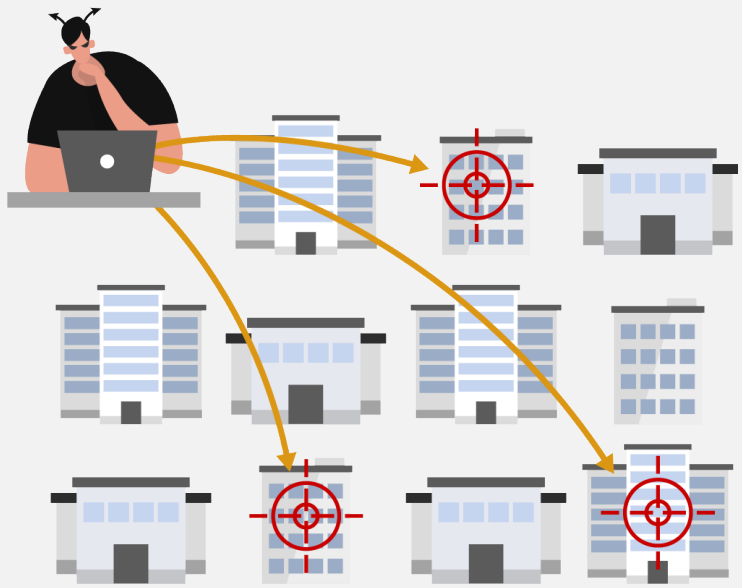
AMIYA

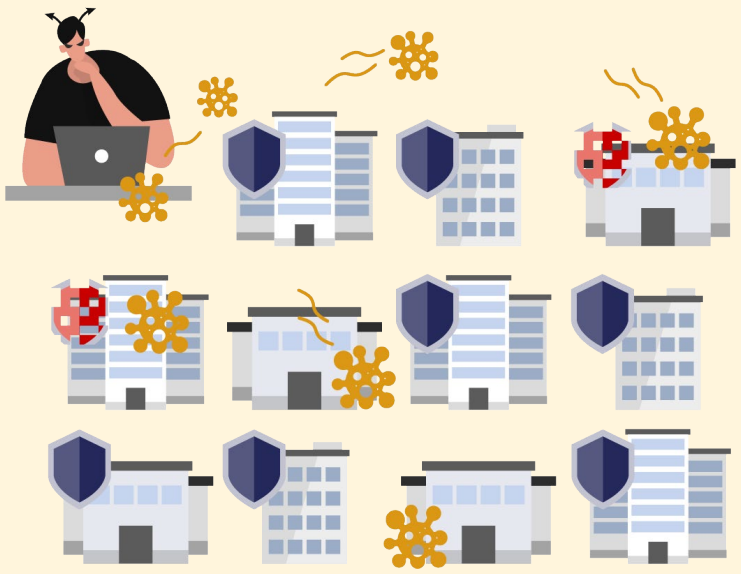
CSIRT構築支援サービス

サイバー攻撃トレンドの変化

特定組織をターゲット&計画的に攻撃



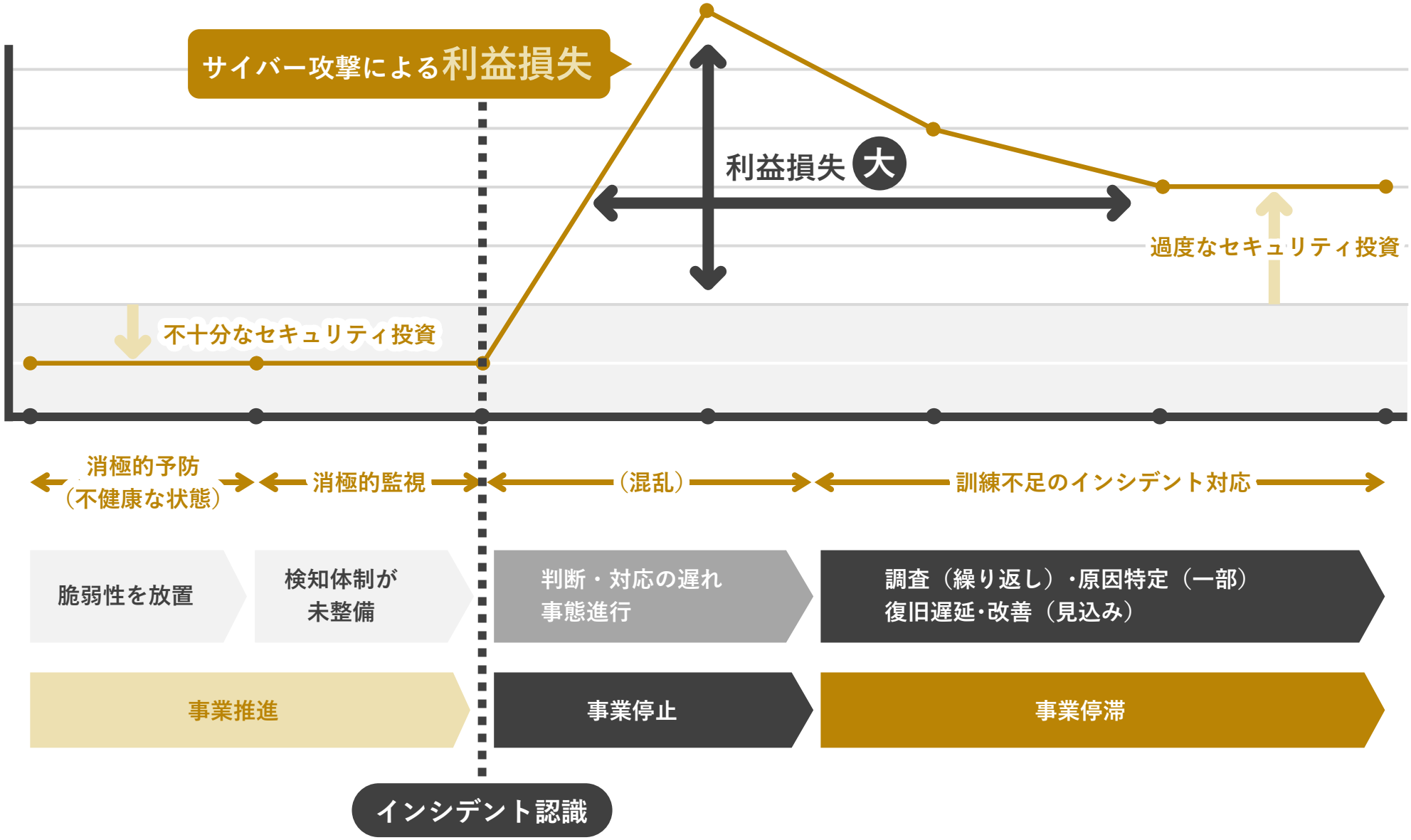
脆弱性のある組織を自動探索&ターゲット



ランサムウェア被害件数は2年で5.5倍に※

※ 出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

サイバー攻撃対応能力不足による利益損失



サイバー攻撃は脆弱性から始まる

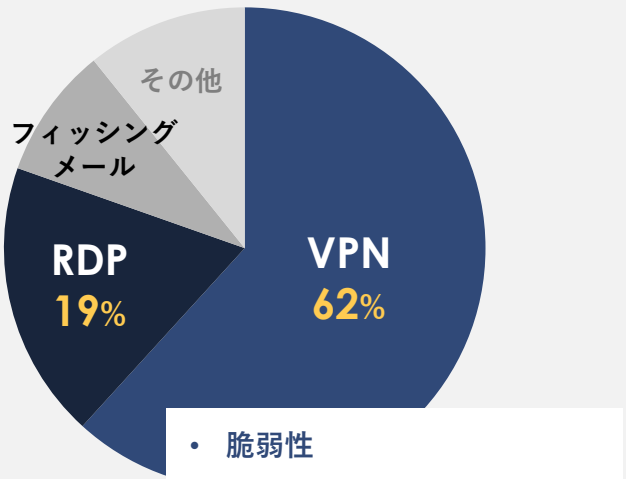
”人やシステム“の脆弱性を狙うサイバー攻撃

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等のニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化（アンダーグラウンドサービス）

脆弱性が原因

出典：独立行政法人情報処理推進機構 (IPA) 情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/files/000108838.pdf

ランサムウェアの侵入経路



- 脆弱性
- 認証強度の弱さ（設定不備）
- 不必要な公開（設定不備）

※ 出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

弱点を無くし、被害発生を抑制する

侵入されることは当たり前

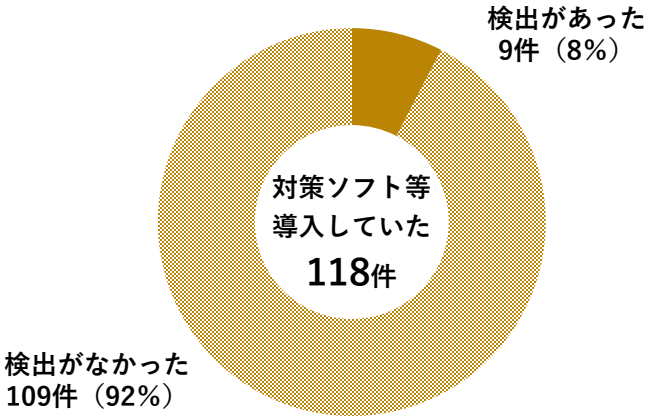
メールからウイルス感染 誰かは開いてしまう

標的型攻撃メール訓練開封率

2021年度		2022年度
約15%	▶	約12%

※出典 東京商工会議所
「「標的型攻撃」メール訓練 実施結果」

ランサムウェア被害時の ウイルス検出率※

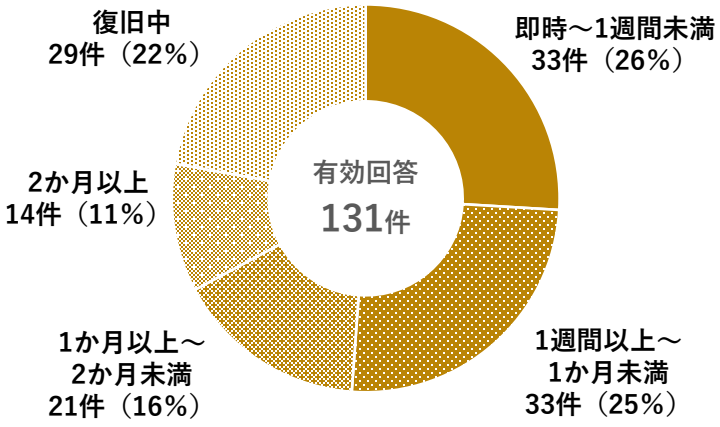


※出典 警察庁「令和４年における
サイバー空間をめぐる脅威の情勢等について」

被害に気づき、大きくなる前に消化する

スピーディなインシデント対応が被害を最小化

ランサムウェア被害の約50%以上が復旧に1ヶ月以上要する※

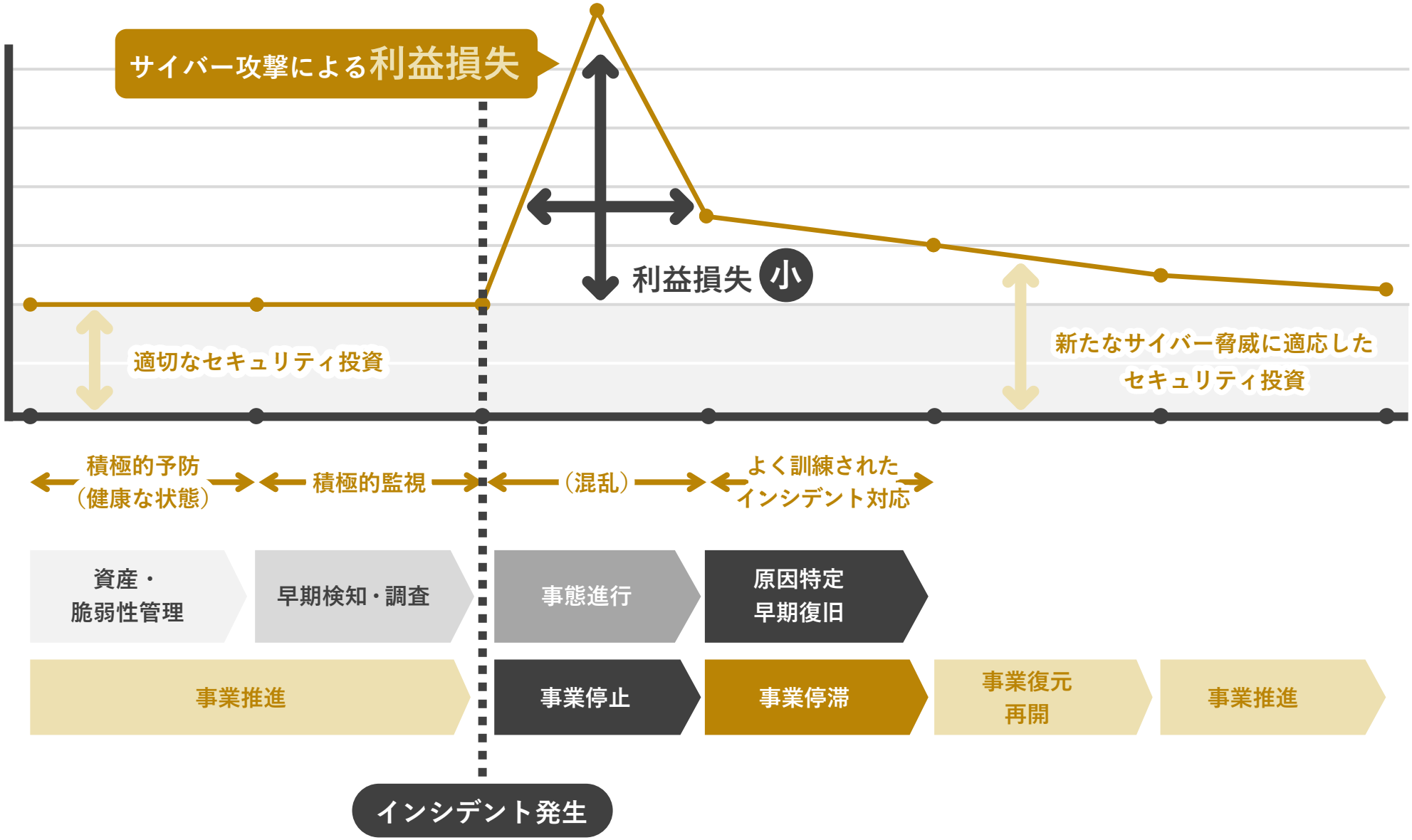


インシデント対応フロー

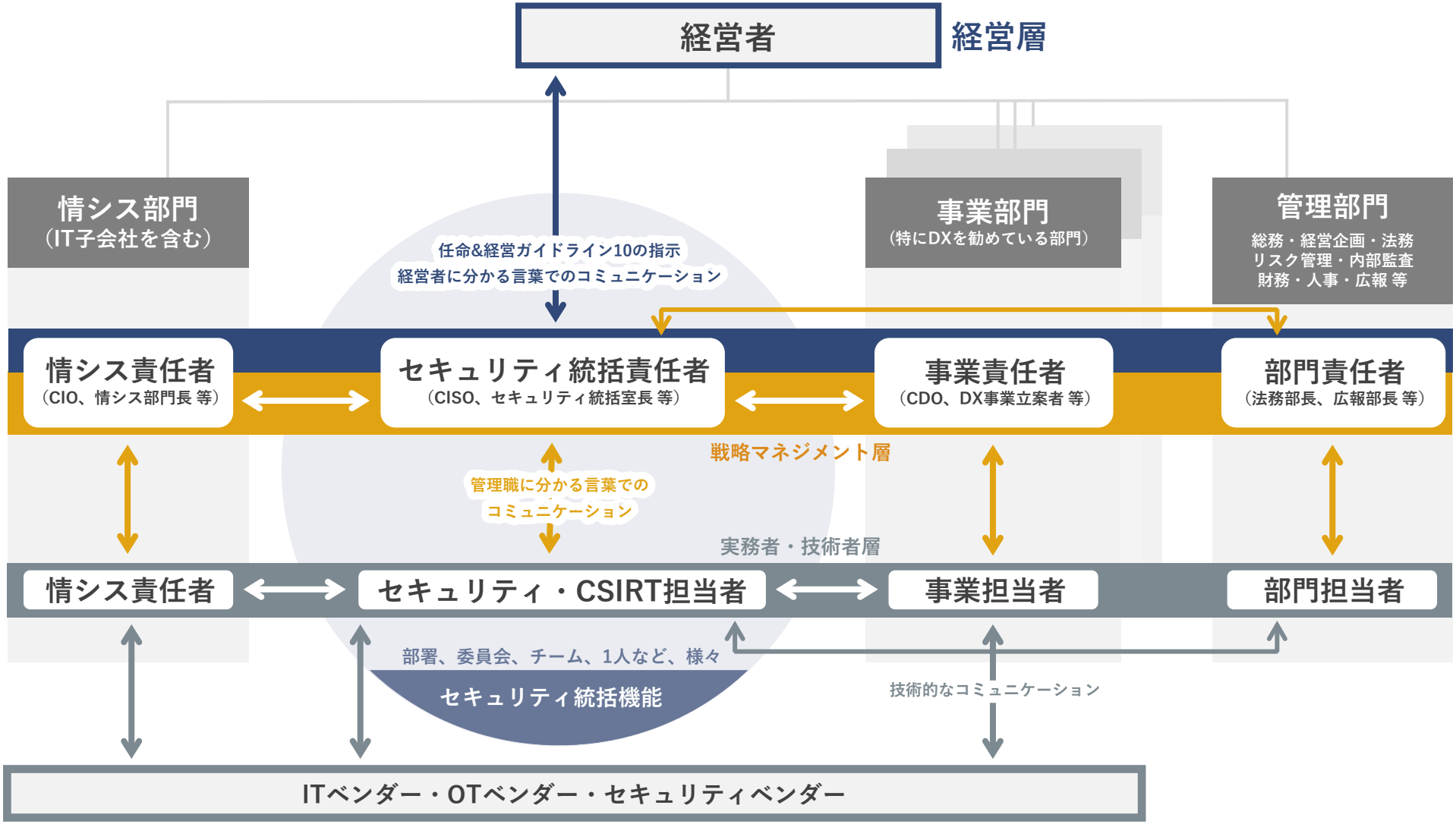
フェーズ1 調査	フォレンジック調査等で原因究明、感染端末の特定 漏洩情報の拡散状況を確認（ダークウェブ調査）
フェーズ2 復旧	復旧計画の作成/ハンドリング支援 （バックアップからの復旧計画等）
フェーズ3 恒久的対応	恒久的なセキュリティ対策を支援 （CSIRT構築やEDR/SOC導入など）

事前準備なしではうまく動けない

セキュリティ対応組織「CSIRTの役割と必要性」



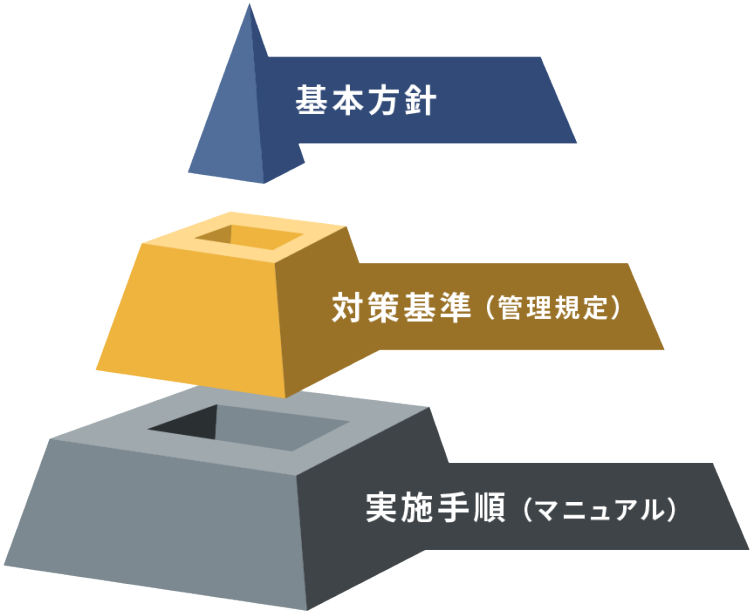
セキュリティ統括機能の設置



※ 出典：経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構 築・人材確保の手引き 第2版」

“組織”としてのセキュリティ対策

ポリシーによるセキュリティ統制



実行組織の確立と運用

ドキュメントの整備による組織の明文化

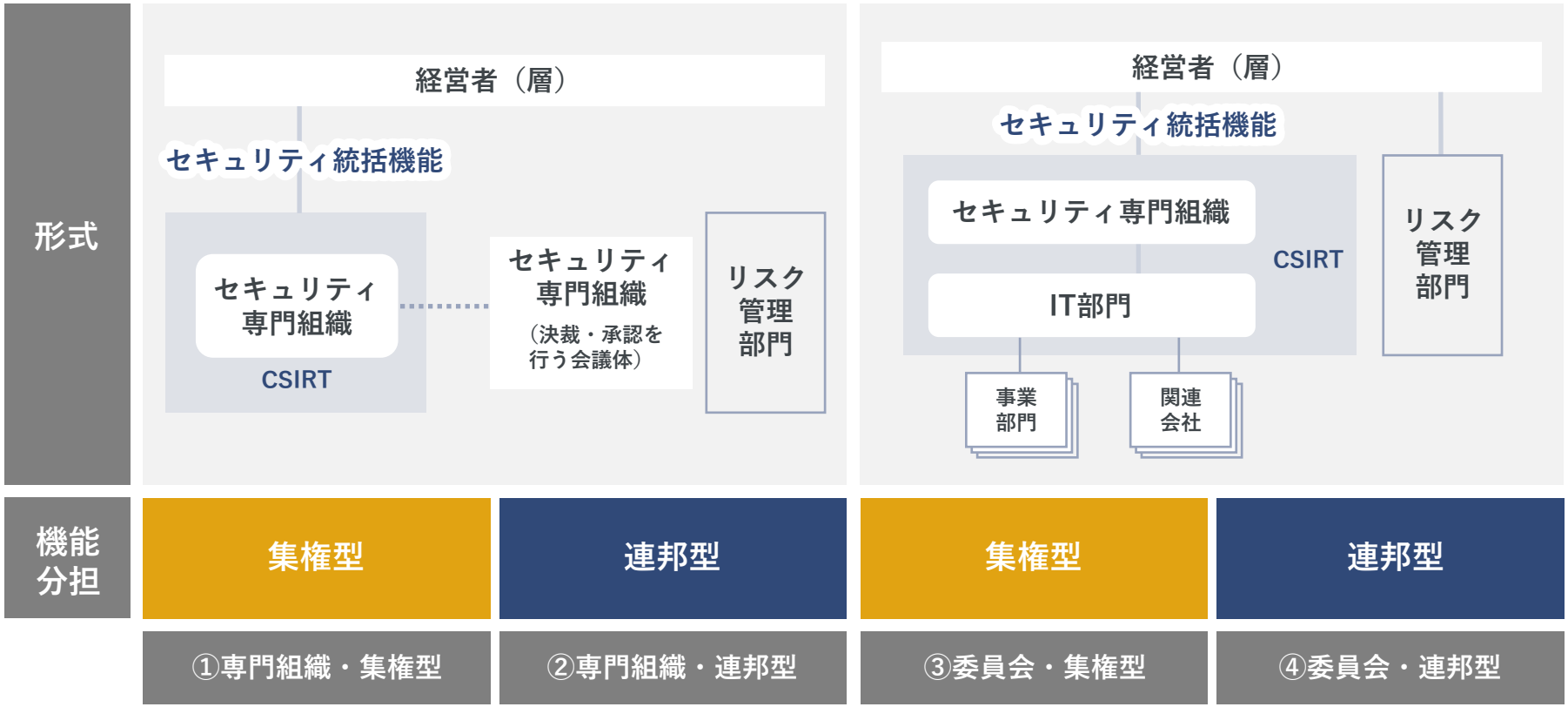
CSIRT構築の流れとサービス範囲

サービス範囲

プロジェクトの立上げ	• 目的の明確化（CSIRT構築のきっかけ） • プロジェクト構成メンバーのアサイン • スケジューリングや運用ルールの明確化、意思決定フローの確認
現状・問題把握	• 現状の情報を収集（既存の体制や守るべき資産、脅威等の把握） • 問題の洗い出し（提供すべきサービスやCSIRTの配置組織、規模感等）
CSIRT構築計画・構築	• CSIRT構築計画書の作成 • 経営層/意思決定層の承認とリソースの確保 • CSIRT体制整備と必要文章の作成、社内説明
CSIRT運用前準備・開始	• インシデントシナリオの作成と机上シミュレーション • 社内/社外への周知、CSIRTサービスの提供開始 • 社外連携体制の確立
再検討	• CSIRT活動の分析 • ポリシーやマニュアル、提供サービスの見直し

CSIRT組織の設置型の検討

自組織のあったCSIRT設置場所を選択する。



※ 出典：経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構 築・人材確保の手引き 第2版」

CSIRTの提供サービスの検討

CSIRTが提供するサービス（自社提供、外部専門組織提供）を決定する。

- セキュリティ対応組織運営
- 即時分析（リアルタイム監視）
- 深掘分析（フォレンジック）
- インシデント対応
- セキュリティ対応状況の診断と評価
- 脅威情報の収集及び分析と評価
- セキュリティ対応システム運用・開発
- 内部統制・内部不正対応支援
- 外部組織との積極的連携

各種ドキュメントの作成

CSIRT規程やマニュアル、インシデント対応フロー、説明会資料のドキュメントを作成。

CSIRT 規定

株式会社 XXX

1．プロジェクトの目的とゴール

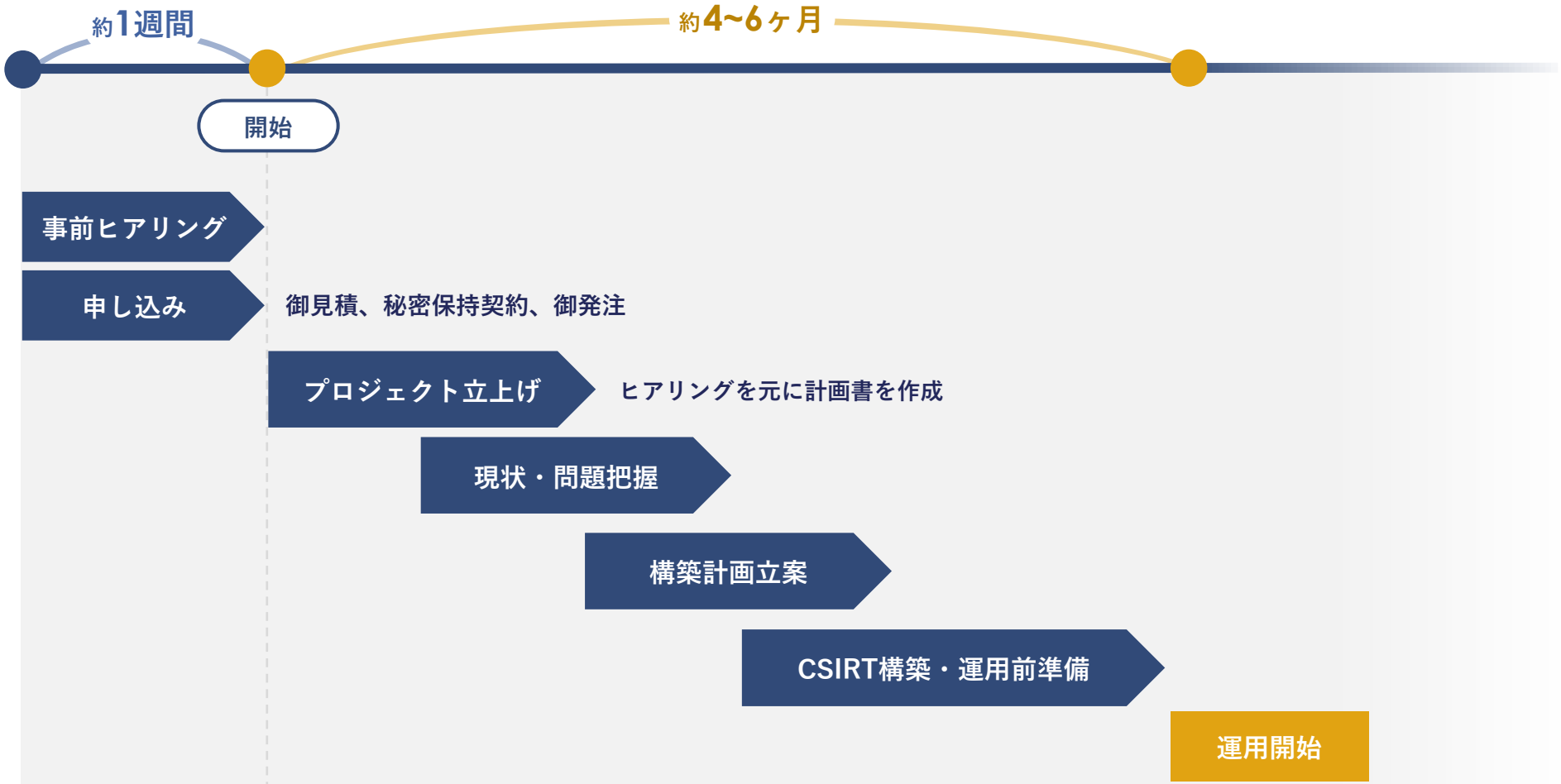
	実施内容
目的	高度化・巧妙化を繰り返している昨今のサイバー攻撃に対抗するためには、ITによる検知・分析機能の導入という技術的対策だけではなく、インシデント対応体制・手順の明確化といった組織での対応体制が必要とされています。 本プロジェクトでは、すでに活動しているCSIRTを整備し、後続のインシデント対応訓練と合わせ、網羅の情報セキュリティレベルを向上させることと共に自社サービス（CSIRT構築）提供のためのノウハウを蓄積することを目的とします。
ゴール	本プロジェクトでは、実用的なCSIRT体制整備を実施するため、まず現状調査を行い、インシデント対応を中心とした課題の洗い出しを行います。 その上で、既存文書との整合性を保ちつつ、CSIRT運営に必要な規程、要領、インシデント対応基本フロー等の文書案を整備します。
アウトプット	①CSIRT規程 ⇒セキュリティインシデント対応方針、CSIRTの目的・対象範囲・体制及び役割・活動内容等を記載したもの。 ②CSIRTマニュアル ⇒セキュリティインシデントの検知・報告・受付、初動対応、被害防止対応等といったCSIRTの活動詳細を記載したもの。 ③インシデント対応フロー ⇒セキュリティインシデントの受付から初動対応、被害防止対応等の各フェーズごとの各関係者の対応内容と順序を示したもの ④説明会向け資料

1

2．対応フロー：検知・報告

2

スケジュール



※監査対応範囲等により、スケジュールは前後します。

包括的な情報システム業務を、月額固定で。

クラウド情シスサービス
ランサポ

『ランサポ』は、お客様の情報システム業務全般をクラウドから代行／支援するサービスです。
エンジニアを派遣しない、低コストかつハイパフォーマンスなクラウド情シスサービスです。

以下のすべてに月額固定で対応します。

サーバ、ネットワークの運用/監視業務
ドキュメント整備・更新、死活監視、保守管理、月次レポート

障害/トラブル対応
サーバ、ネットワーク、クラウド、PCなどに対する問い合わせ対応及び障害対応

定型業務代行
アクセス権申請対応、アカウント管理ポリシー管理、設定変更など

PCマスターイメージ作成
PCマスターイメージの作成・定期更新

年間計画の作成支援
次年度の予算やロードマップ作成を支援

BCP関連支援
リスクレベルに応じたBCP対策を支援

クラウド移行支援
最適なクラウドの選定や移行方法などを支援

セキュリティ対策支援
今後のセキュリティ対策をアドバイス

AMIYA