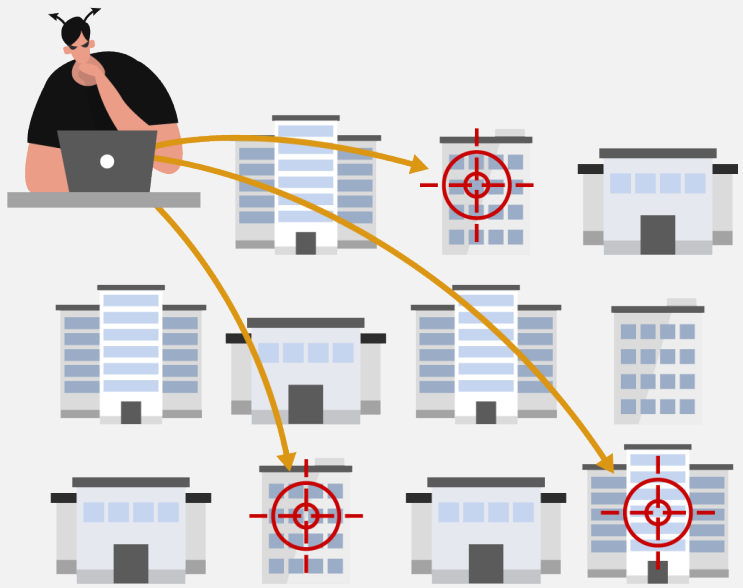
AMIYA

セキュリティ監査サービス

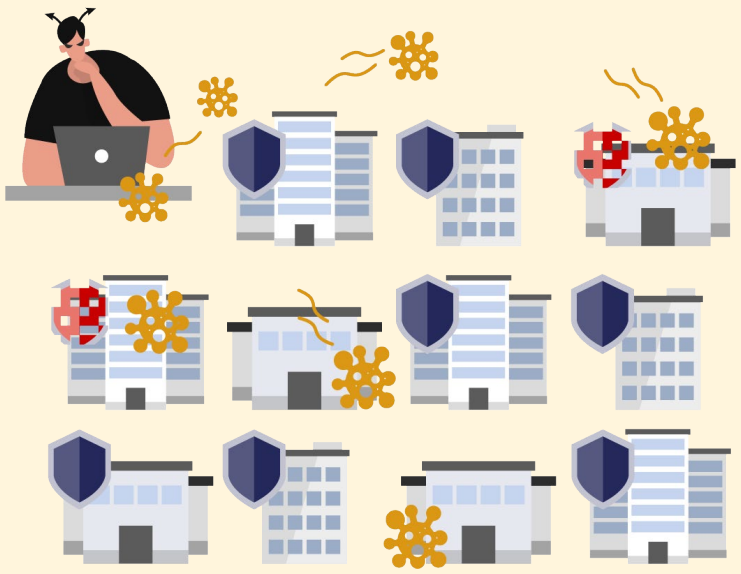
(C) AMIYA Corporation

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」

(C) AMIYA Corporation

サイバー攻撃は脆弱性から始まる

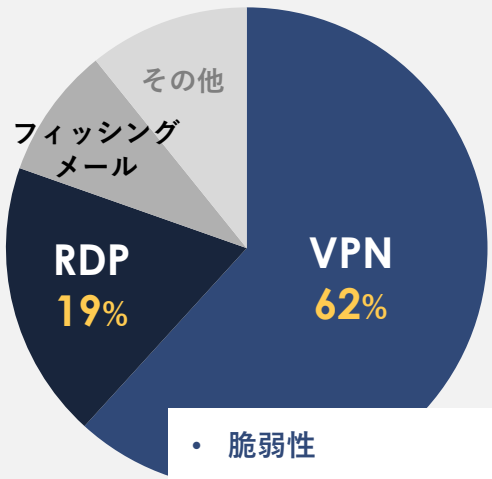
”人やシステム“の脆弱性を狙うサイバー攻撃

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）

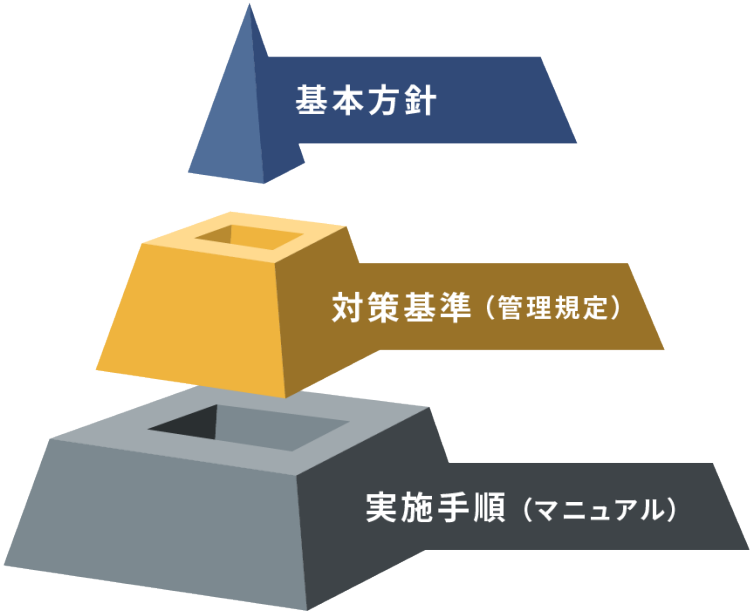
※ 出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

セキュリティツールを導入しても、脆弱性や設定不備を放置したままでは一発アウト

(C) AMIYA Corporation

“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

組織のセキュリティ成熟度を向上

(C) AMIYA Corporation

組織のセキュリティ成熟度の“今”を知る

組織の課題を明確化し、今後の目標の設定とそれに向けた実行が大切

- 組織の資産のインベントリ管理
- ソフトウェア資産のインベントリ管理
- データ保護
- 組織の資産とソフトウェアの安全な構成
- アカウント管理
- アクセス制御管理
- 継続的な脆弱性管理
- 監査ログ管理
- 電子メールとWebブラウザの保護
- マルウェアの防御
- データ復旧
- ネットワークインストラクチャ管理
- ネットワークの監視と防御
- サービスプロバイダーの管理
- アプリケーションソフトウェアセキュリティ
- インシデントレスポンスと管理

※ CIS Controls v8から抜粋

(C) AMIYA Corporation

サイバーハイジーンの効果

サイバーハイジーン対応※1は、ランサムウェア攻撃手法※2の78%に効果的

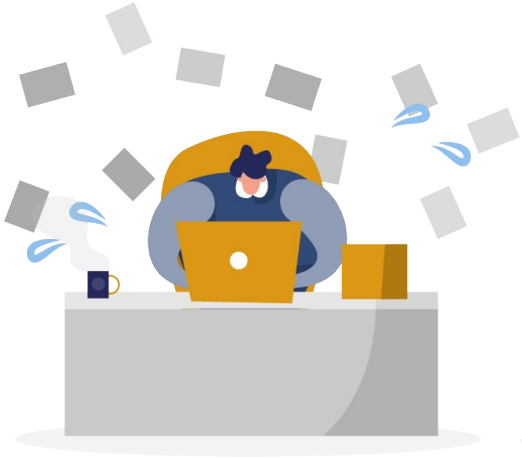
	基本的なハイジーン対応（56の保護手段※1）	包括的なセキュリティ対応（153の保護手段※3）
マルウェア	77%	94%
ランサムウェア	78%	92%
Webアプリケーションのハッキング	86%	98%
内部関係者の特権悪用	86%	90%
標的型侵入	83%	95%

出典：CIS Community Defense Model Version 2.0
https://learn.cisecurity.org/Community-Defense-Model-v2.0

※1 CIS Controls v8 IG1
※2 MITRE ATT&CKフレームワークのATT&CK（サブ）技術
※3 CIS Controls v8 IG3

(C) AMIYA Corporation

自組織内で実施できない要因



人材の不足

対応できる人材がいない
セキュリティ新情報の収集が大変

独立性の欠如

組織内のパワーバランスが影響

客観性の欠如

思いこみや利益相反が影響

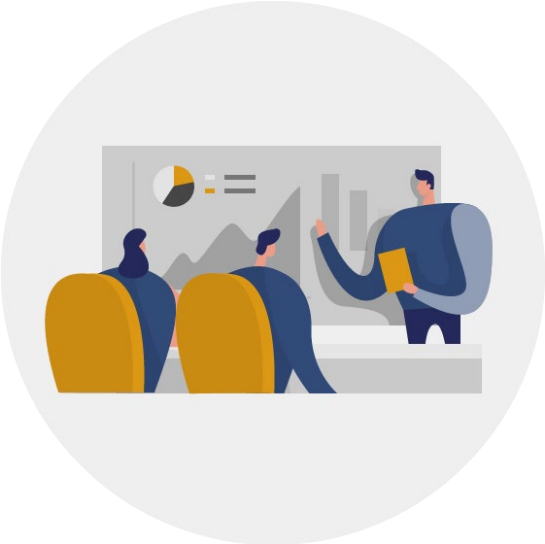
(C) AMIYA Corporation

セキュリティ監査サービス

公的資格を有するセキュリティスペシャリストがポリシーやレギュレーションへの対応状況をチェックする監査サービスです。
セキュリティリスクを洗い出し、今後の対策へ繋げることで、組織のセキュリティレベルを向上します。

公的資格を有する セキュリティスペシャリスト

- CISA（公認情報システム監査人）
- 情報処理安全確保支援士



ギャップ分析/評価

- セキュリティポリシー
- 各種ガイドライン（ISO/IEC 27001等）
- 対応の実態

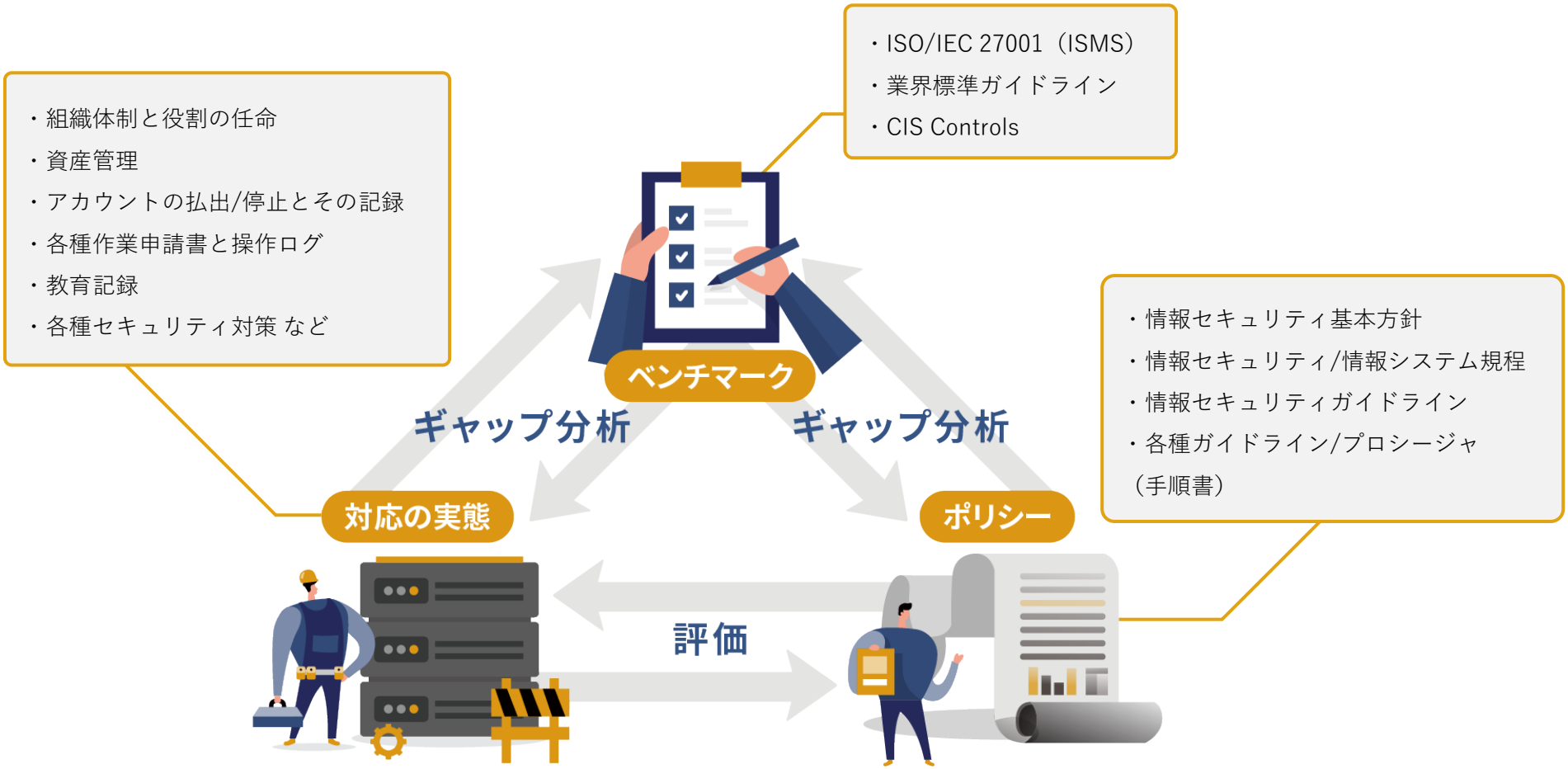
レポート/報告会

- 監査チェックリスト
- 監査計画書/報告書
- ポリシー改定案

(C) AMIYA Corporation

組織のセキュリティ課題を見える化

ベンチマーク（レギュレーション）を軸に、「組織のポリシー」および「対応の実態」とのギャップを分析します。
ギャップ/評価を見える化することで、今後の改善につながります。



(C) AMIYA Corporation

ギャップをチェックリストで確認

ベンチマーク（レギュレーション）とのギャップを分析し、調査結果としてチェックリストを提供します。
これを元に今後の改善策を検討します。

監査チェックリスト例

No.	監査項目	基準等の項番	監査手続	収集すべき証拠資料	規定・推奨	留意点	監査証拠	監査メモ
ISMSの適用範囲								
マ-1	ISMSの適用範囲及び境界が明確に定義されていること。	4.2.1 a)	①適用範囲が定義され、文書化されているかどうか確かめる。	・適用範囲定義	○			
			②以下の観点から、ISMSの適用範囲が定義されているかどうか確かめる。 ・事業の特徴 ・組織 ・組織の所在地 ・資産 ・技術	・適用範囲定義	○	文書への記載と図面の一致をチェックすること。		
			③適用範囲の境界線が明確かどうか確かめる。	・適用範囲定義	○	①物理的な境界線をチェックすること。 ②論理的な境界線をチェックすること。		
ISMS基本方針の策定								
マ-2	ISMS基本方針が策定されていること。	4.2.1. b)	①ISMSの基本方針が定められているかどうか確かめる。	・ISMS基本方針定義	○			
			②以下の観点から、ISMSの基本方針が定められているかどうか確かめる。 ・事業の特徴 ・組織 ・組織の所在地 ・資産 ・技術	・ISMS基本方針定義	○			
			③目的を設定するための枠組みが含まれ、情報セキュリティに関する全般的な方向性及び行動指針が確立されているかを確かめる。	・ISMS基本方針定義	○			
			④事業上の要求事項や法的又は規制要求事項、並びに契約上のセキュリティ義務が考慮されているか確かめる。	・ISMS基本方針定義	○			
			⑤ISMSを確立し、維持するために必要な戦略上の視点からみた組織環境、ならびにリスクマネジメントのための環境が整備されているかどうかを確かめる。	・ISMS基本方針定義 ・ISMSマネジメント体制	○			
			⑥リスクを評価する上での基準が確立されているか確かめる。	・ISMS基本方針定義	○			
			⑦経営陣による承認がなされているかどうかを確かめる。	・ISMS基本方針定義	○			

1ページ

(C) AMIYA Corporation

ポリシー改訂でギャップを埋める

ベンチマーク（レギュレーション）とポリシーのギャップを元に、ポリシー改訂案を作成します。
また、新たにポリシーの作成が必要な場合は、ポリシー案を作成します。

ポリシー新旧対応表例

情報機密管理規定

	旧	新	備考
第２章 情報機密管理			
第５条（情報機器の管理運用）	情報機器等の取扱者は、情報機器等、また情報機器等に記録された情報の不正利用等がないよう、万全を期さなければならない。 ①情報機器等の取扱者は、情報機器等の第三者による不正使用等がないよう、携帯可能な情報機器等の保管には相当な注意を払わなければならない。 ②取扱者個人の判断による会社所有の情報および機器等の持ち出しを禁止する。持ち出す場合は、所定の手続きに従う事とする ２ 個人所有の情報機器、ソフトウェア、情報・データの会社への持ち込みを禁止する。	変更なし	
第６条（ソフトウェアの管理運用）	定められた標準パッケージソフトウェア以外のソフトウェアを使用（インストール）してはならない。 別途定める標準パッケージソフトウェア=社内標準インストールソフト：「社内標準ソフトウェア一覧」を参照 ２ 情報機器等の取扱者は情報機器等の健全な利用と法令遵守に努めなければならない。 ３ 市販ソフトウェアを使用する際は、当該ソフトウェアの使用権許諾契約の内容、著作権の取扱い、特にコピー等の制限、禁止事項について充分確認し、遵守しなければならない。 ①購入したソフトウェア本体やマニュアル類は、所在を明確にして管理しなければならない。 ②コンピュータウィルス感染の予防の為、感染の恐れがある以下に定める行為を行ってはならない。 1)市販ソフトウェアの使用権許諾契約、著作権に反するコピー、及びその使用 2)出所不明ソフトの使用 3)社外ネットワーク経由のソフトウェア及び疑わしき情報の取得 4)情報機器等がコンピュータウィルスに感染していることを発見した者は、別途定める「DK-003ウィルス感染防止ルール」に従わなければならない。		3)社外ネットワーク経由のソフトウェア及び疑わしき情報の取得 →正規の販売店が運営するウェブサイトや正式な運営元の提供サイト以外からのソフトウェア及び情報の取得

(C) AMIYA Corporation

ポリシーと実態の差分を確認/是正

「組織の情報セキュリティポリシー」と「対応の実態」との評価結果を監査報告書として提供します。
ポリシーに促していない実態の改善に繋げます。

監査報告書例

ISMS 内部監査報告書

（文書番号：　　）

●●株式会社

承認	情報セキュリティ委員会（確認）	内部監査責任者
㊞	㊞	㊞
2006 年 12 月 31 日	2006 年 12 月 31 日	2006 年 12 月 31 日

●●株式会社		様式名	ISMS 内部監査報告書	ページ	3/5
文書番号		作成日	2006 年 12 月 31 日	機密区分	社外秘

2．ISMS 内部監査結果サマリ

この度の ISMS 内部監査におきましては、ISMS の整備状況、ISMS の構築におけるこれまでの活動、並びに ISMS の理解度の監査を中心に進めてまいりました。ISMS 整備状況、並びに ISMS 構築におけるこれまでの活動につきましては、ISMS 文書やこれまで作成されてきた記録の確認及び、情報セキュリティ委員会事務局へのインタービューから、ISMS 構築のために適切な活動がなされ、ISMS が十分に整備されていることを確認致しました。

また、各被監査部門の部門責任者、並びに業務担当者へのインタービューから、ISMS のための教育が十分になされ、今後 ISMS を運用・維持・改善できるだけの理解度があることを確認致しました。

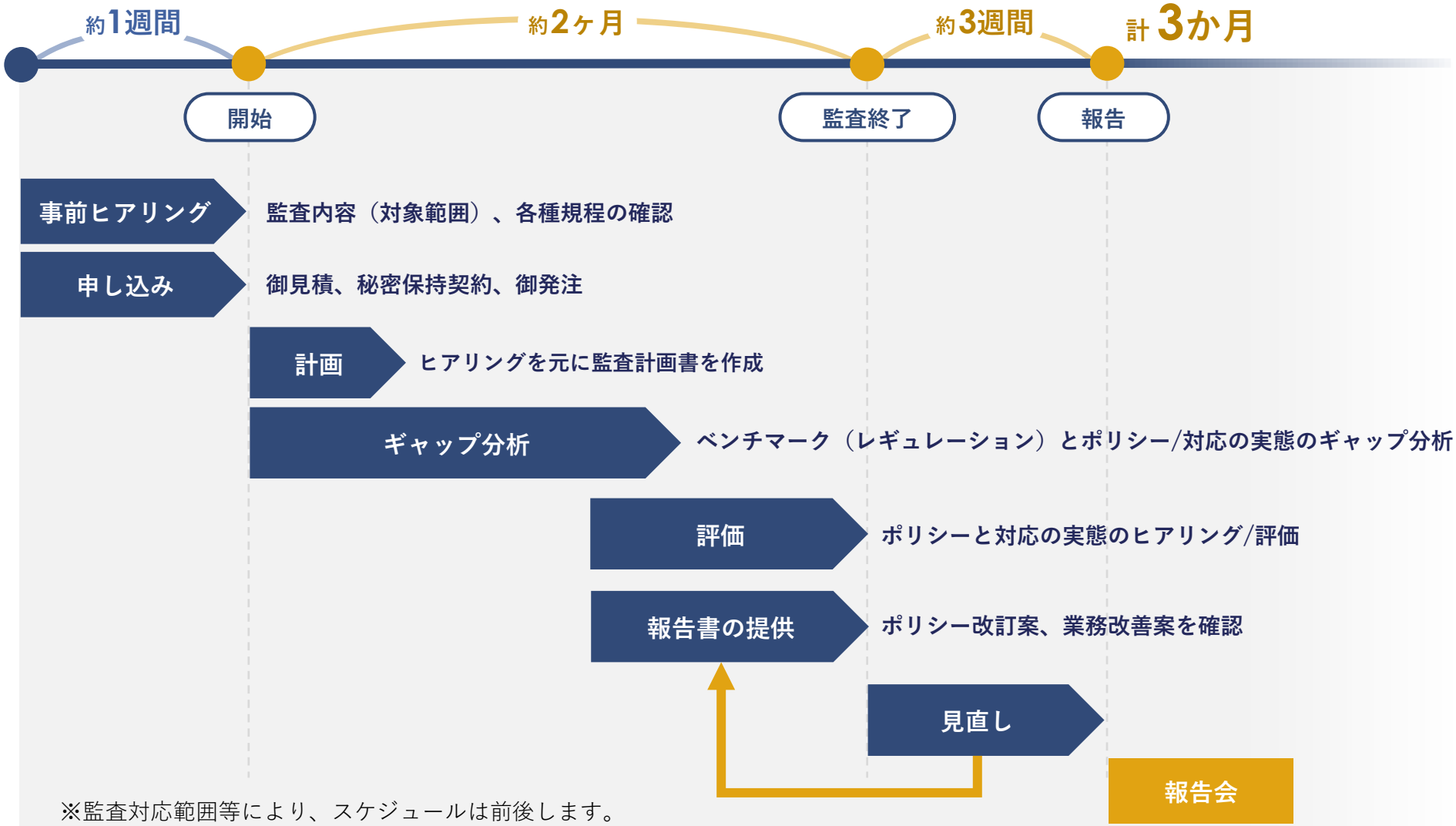
ISMS 内部監査実施の結果と致しまして、全体を通じて重大な不適合は発見されませんでした。軽微な不適合事項につきましては、●件、観察事項につきましては、●件、大変評価できる事項（Good Point）につきましては、●件確認致しました。

尚、軽微な不適合事項、観察事項、大変評価できる事項（Good Point）それぞれにつきましては、下表のような対応が望まれます。

区分	望まれる対応
軽微な不適合事項	不適合の事項ですので、速やかに是正計画を立案し、是正することが望まれます。
観察事項	観察事項は、不適合の事項ではありませんが、将来的に不適合の原因となる可能性があるため、情報セキュリティ委員会等、組織の中で、是正の必要性を検討し、必要があれば、是正することが望まれます。
大変評価できる事項（Good Point）	工夫が見られ、非常に効果的な活動や運用がなされていると判断できる事項ですので、今後も該当する活動や運用を継続されることが望まれます。

(C) AMIYA Corporation

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。

(C) AMIYA Corporation

選べるコンサルティング・監査サービス

情報セキュリティや情報システムの管理体制の確立をはじめ、ITガバナンスへの対応に必要となる、
「文書化」「教育・研修」「監査・認証取得」など、様々なコンサルティングサービス、監査サービスを提供します。

情報セキュリティ管理	個人情報保護	ISMS認証	Pマーク認定取得
CSIRT構築	危機管理体制	ITガバナンス	J-Sox対応

体制確立
リスク/課題の分析・評価

- リスク管理体制構築支援
- リスクアセスメント支援
- ビジネスインパクト分析支援
- リスク対応支援

文書化
教育/研修・運用

- 文書策定支援
- 教育コンテンツ作成支援
- 教育・研修実施支援（講師代行）
- アドバイザリー支援
- 緊急時対応計画策定支援
- 緊急時対応の教育・訓練支援

監査・改善措置

- 監査体制構築支援
- 監査員教育支援
- 文書/実地監査支援
- 改善/再発防止対応支援

(C) AMIYA Corporation

サンプル費用

自工会/部工会・サイバーセキュリティガイドライン対応

業種：製造業（部品メーカー）
会社規模：４拠点/300名
監査範囲：全社
金額：300万円

情報セキュリティ内部監査態勢の整備

業種：卸売業
会社規模：200名
監査範囲：全社
金額：150万円

新規上場に向けたIT全般統制対応

業種：情報・通信業
会社規模：200名
監査範囲：J-Sox対象システム
金額：500万円

自治体ネットワーク強靭化対応

業種：地方自治体
会社規模：250名
監査範囲：ITシステム全体
金額：350万円

金融商品取引業者等のシステムリスク管理態勢対応

業種：金融商品取引業
会社規模：150名
監査範囲：ITシステム・クラウド全体
金額：380万円

ISO/IEC 27001認証取得対応

業種：その他製造業（リサイクル）
会社規模：100名
監査範囲：2拠点（工場）
金額：200万円

(C) AMIYA Corporation

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

(C) AMIYA Corporation

AMIYA

(C) AMIYA Corporation