テーマ2：

# 内部監査を有効に運用するための手法の考察

日本ISMSユーザグループ
インプリメンテーション研究会

2017年12月13日

副主査　秋山　健一

# はじめに

テーマ2では、研究会参加メンバ各位におけるISMSの運用フェーズの課題が活発に議論されている。
毎年テーマを継続し、より良いISMSに向け課題整理を行っている。

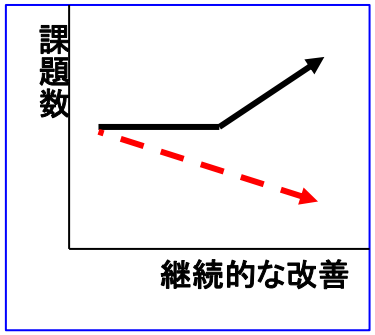
可能な限り、当研究会の成果を本セミナーに参加頂いている各社の事務局や推進者などの皆さまに持ち帰り頂き、自組織の運用フェーズにおける課題のヒントとして頂きたい。

2017年もメンバ各位の間で多種多様な議論が行われた。しかしながら、すべての議論を本書に記載する事には至っていない。
是非とも、本研究会へ参加いただき、実際の議論の場を体験し、自組織の課題解決に繋げて頂ければと思います。

# インプリ研テーマ2の検討経緯　1/2

## 2013年

**ISMS推進各社が抱える諸課題の対応策**

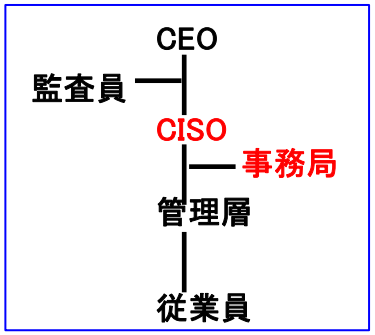



**運用を継続しても課題は減少しない**

**「人」が原因**

## 2014年

**ISMS推進事務局の悩みと解決策**

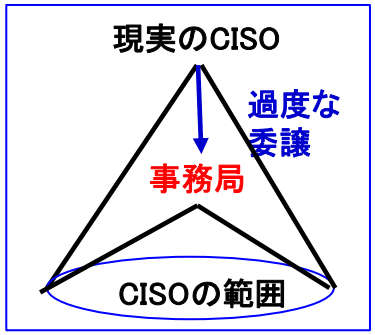



**事務局自身が機能不全是正不可に**

**CISOと事務局の「役割」が不明確**

## 2015年

**ISMSを成功させるためのCISOの条件**

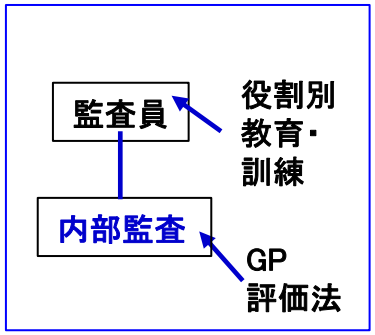



**規格の要求事項はCEOからCISOへ委嘱**

**CISO機能の事務局への過度な「委譲」**

## 2016年

**運用フェーズにおける有効性の評価**




**時間経過によりISMSの有効性が低下**

**内部監査のマンネリ化**

# インプリ研テーマ2の検討経緯　2/2

2016年のテーマ2では「ISMSの有効性の低下」に着目し、

- その一現象である「内部監査のマンネリ化」が発症していないかを検出する手法
- マンネリ化防止策としての、
  - 監査員を中心とした役割別教育・訓練等による力量の確保
  - GoodPoint評価法による内部監査

について議論した。

これを受け2017年度テーマ2では、マンネリ化防止後の次なるステップとして**「内部監査を有効に運用するための手法の考察」**をテーマとし、課題の整理・対策検討・具体的な対応例を提示していく。

# 2017年度テーマ2のねらい

**ISMSの年間活動の中で、内部監査は年に1回（ほとんどの組織が年に1回）である。その内部監査を有効に運用する手法を検討する。**

**自覚症状が無い大きな病気（不適合）が確実に見つかる有効な診察（監査）としたい。**

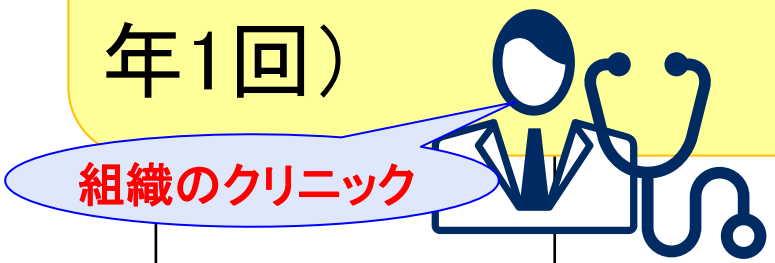
# 現状把握：
# 内部監査の運用事例

# ISMS年間活動スケジュール（例）

## ISMSの年間活動は以下の通り。

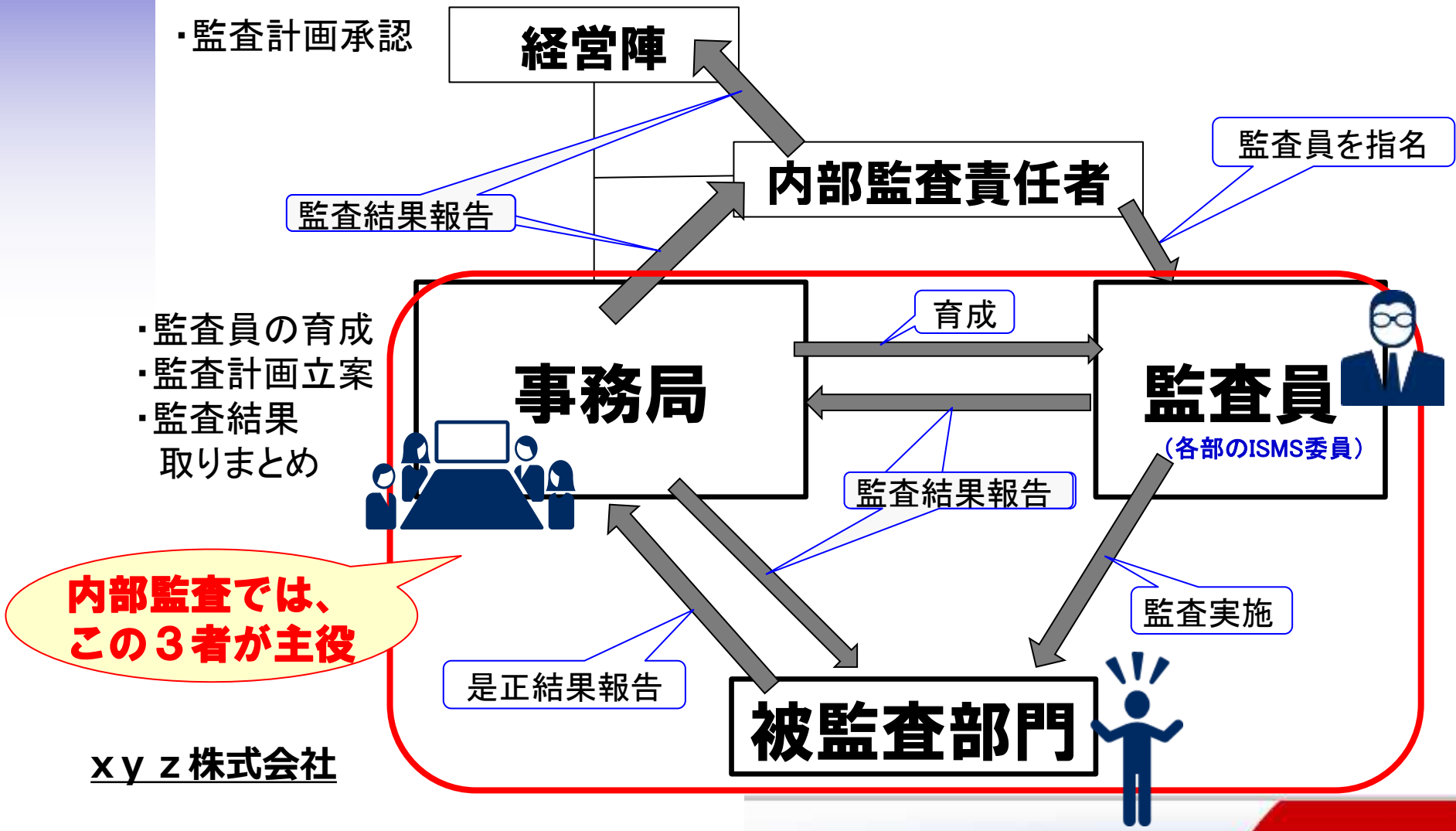
| 1Q | 2Q | 3Q | 4Q |
|---|---|---|---|
| リスクアセスメント | | | |
| リスク対応 | | | |
| | | 内部監査 | |
| | | マネジメントレビュー ☆ | |
| | | | 審査 ☆ |

内部監査は年1回！
（ほとんどの組織は年1回）



# 内部監査に関わる組織（例）

・事務局が取りまとめ（内部監査員の育成、監査計画、監査結果報告など）
・各部推進者によるクロス監査　　・実施頻度：年1回




xｙｚ株式会社

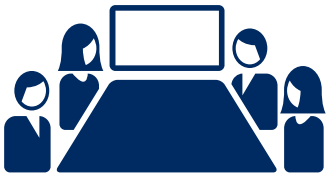
# 何を基にして監査をするか（内部監査の元ネタは何か）

**規格書**

ISO27001

**社内ルール**

・情報セキュリティ対策基準
・持ち出し管理規程
・個人情報保護マニュアル
・企業秘密管理規程
などなど



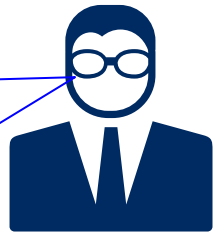
事務局

内部監査員教育
（事務局主催）

・ISMSの規格や社内ルールを基に「内部監査チェックシート」を作成しました！これを使ってください。

**内部監査チェックシート**

Q1. 方針はどのように周知していますか
（回答例：ポスター掲示）
Q2. 部員に対する教育はどうしていますか
（回答例：事務局主催の全社教育を受講）
Q3. ・・・・・



監査員

このチェックシートを全て確認すればいいのだな！

# 課題整理：
# チェックシート方式の問題点

# 内部監査時の監査員の監査ツール比較

| ツール※1 | 採用組織 | ツールの作成者 | メリット | デメリット |
|---|---|---|---|---|
| **規格書、社内ルール** | 少ない<br>※2 | ー<br><br>（社内ルールは事務局） | 事務局の事前準備がなく、事務局は楽 | 監査員は規格書、社内ルールの十分な理解が必要<br><br>監査員のスキルが高くないと規格書等だけで確認するのは厳しい（監査結果は監査員の力量に左右される） |
| **内部監査チェックシート** | 多い | 事務局<br>（規格書や社内ルールを基に作成） | 監査員はチェックシートを基に実施するだけ（監査員のスキルが低くても網羅的には監査できる、監査員は楽） | **チェックシートに記載されていないことは監査員はチェックしない（出来ない）**<br><br>**監査員は事務局に依存してしまい、監査員の育成には効果が低い** |
| **新手法！？** | **（今回、テーマ2では新たな手法を検討する）** | | | |

※1　内部監査時に監査員が使うツール
※2　規格書、社内ルールのみで内部監査をする組織は少ない

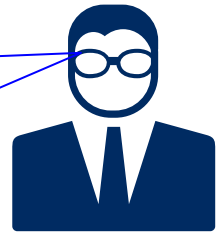
# チェックシートベースの監査における、よく（？）みかける風景

## 被監査部門

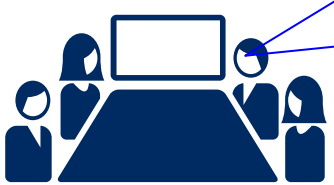
・今年もチェックシートベースで監査される！チェックシートはこれだよな（被監査部門の推進者＝監査員）。事前にこの内容を確認しておけばクリアだ！

## 監査員

・監査など1年ぶりだぞ！事務局がチェックシートを用意している。取りあえずこの通りやればいいか。
・時間は1部門2時間だ。この中で、必須の確認項目は必ず時間内に確認しなければ！



## 事務局



・監査員の育成計画を立案しよう。
・各部から推進者が選出されてきた。内部監査員研修の内容は去年と同じで良いよね。
・そういえば監査のスペシャリストのAさんが異動になったな～

# チェックシート方式での問題点

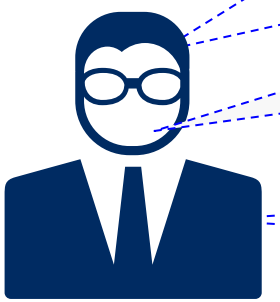
“チェックシート”に記載されていることは確認するが、記載されていること以外は確認しない（書いてないから確認などしない（出来ない））

**・被監査部門の隠れたリスクに監査員は気付かない可能性が高い**
**・監査員はチェックシートに依存するため、力量向上に乏しい**

監査説明会では、必ず必須監査項目（例：委託先管理）はみるように言われていた！あれれ、ヒアリングしたら、この部には委託先が無いじゃないか！当たり前か、ここは営業部だから委託先などないよな～

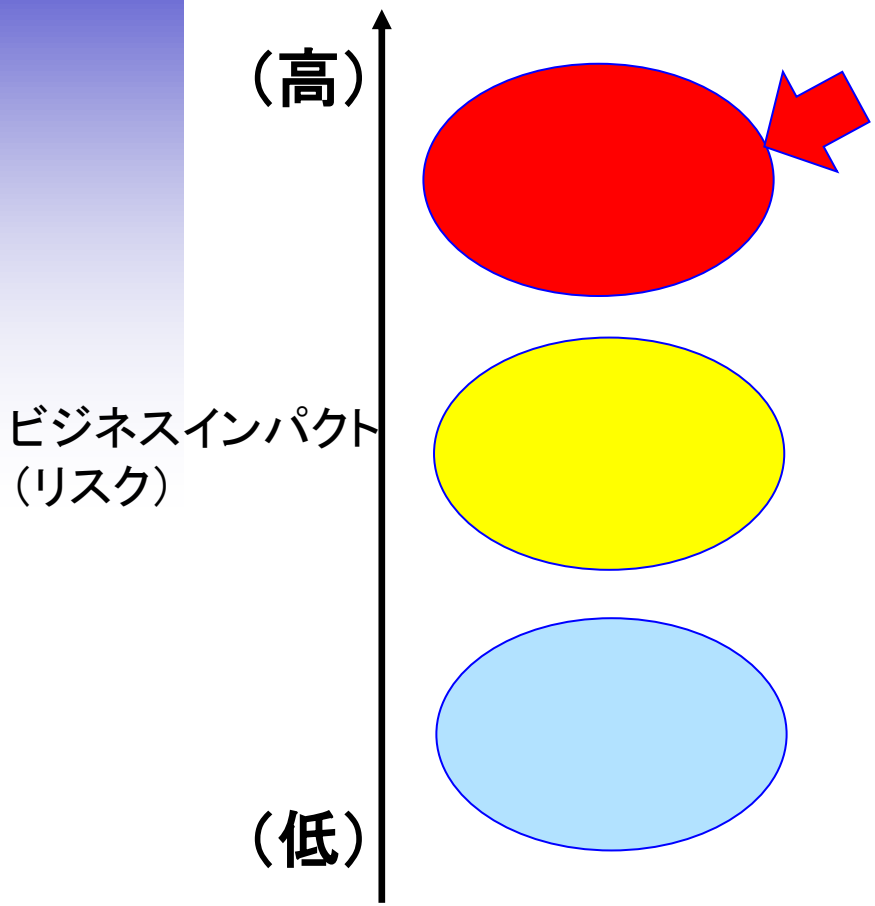
事務局の内部監査チェックシートを基にするとUSBメモリと個人情報の管理状況をみることになっているが、そもそもA開発部にはそれらは無いではないか。時間がムダだった．．

A開発部は、新しい業務（ビッグデータ・AI）を始めたようだ。でも、時間が無いから、確認しなくていいか。チェックシートに書いてないし．．



監査員

# リスクを把握して監査に臨む土台作りが重要




このような領域にフォーカスした監査としたい
（このような領域の監査漏れを防ぎたい！）

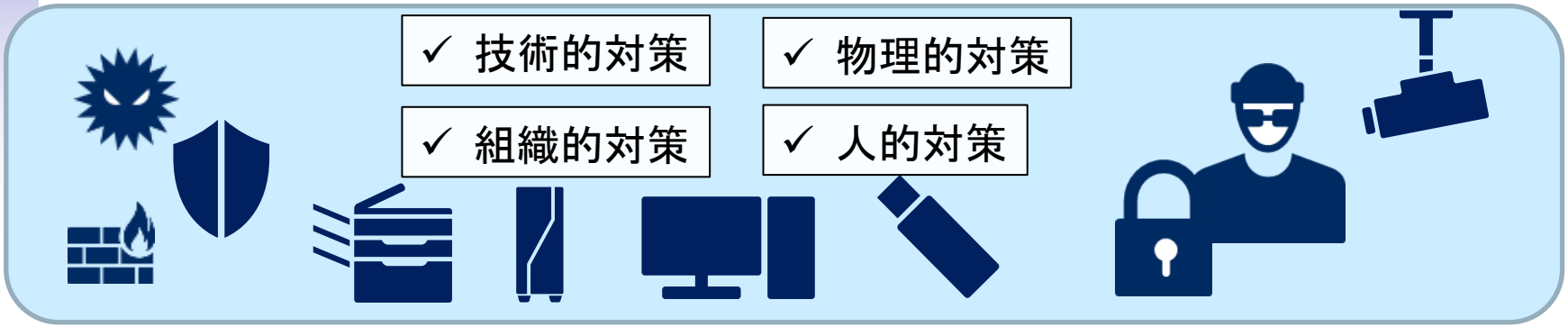
**監査で確実にリスクのある領域を監査させる土台を作る！**

リスクが低いところばかりの監査では、「重箱の隅・・内部監査」になる。その監査結果をもらっても被監査部門に納得感が得られることは少なそう。

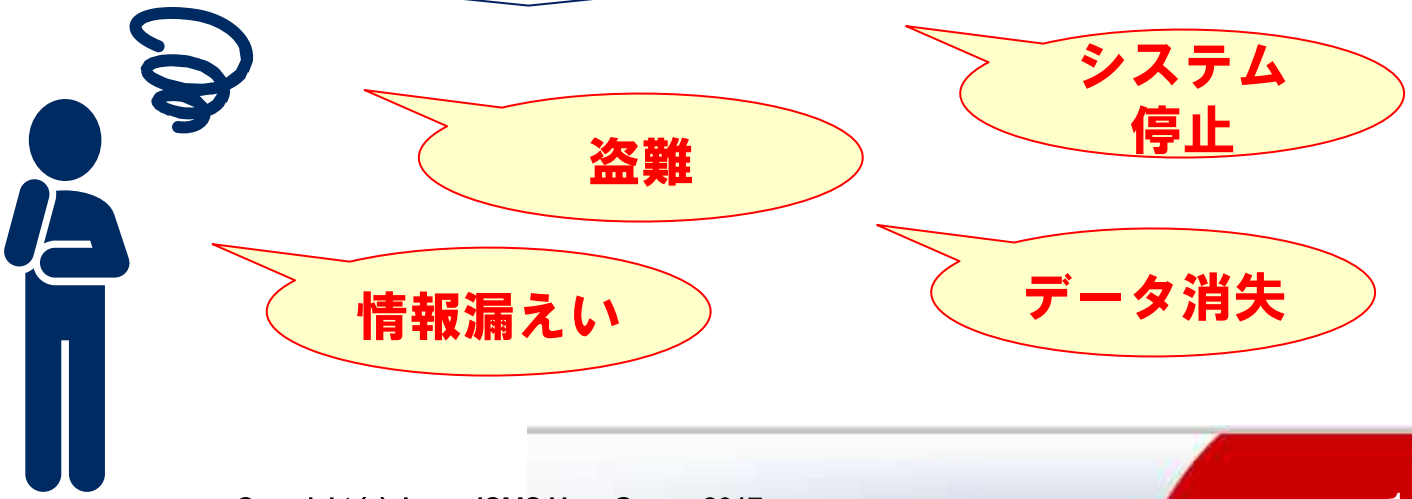
リスクの高いところを監査し忘れて、後で大変になることが無いようにすべき！被監査部門が監査員に対して、見つけてくれて有難うというよう監査とすべき。

# 内部監査では、リスクの高いものを見逃してはならない

ISMS内部監査では、その組織の“高いリスク”を見逃してはなりません。
網羅的に管理策114項目を一つひとつ確認するのではなく、高いリスクを見逃さない仕組み作りが必要である。



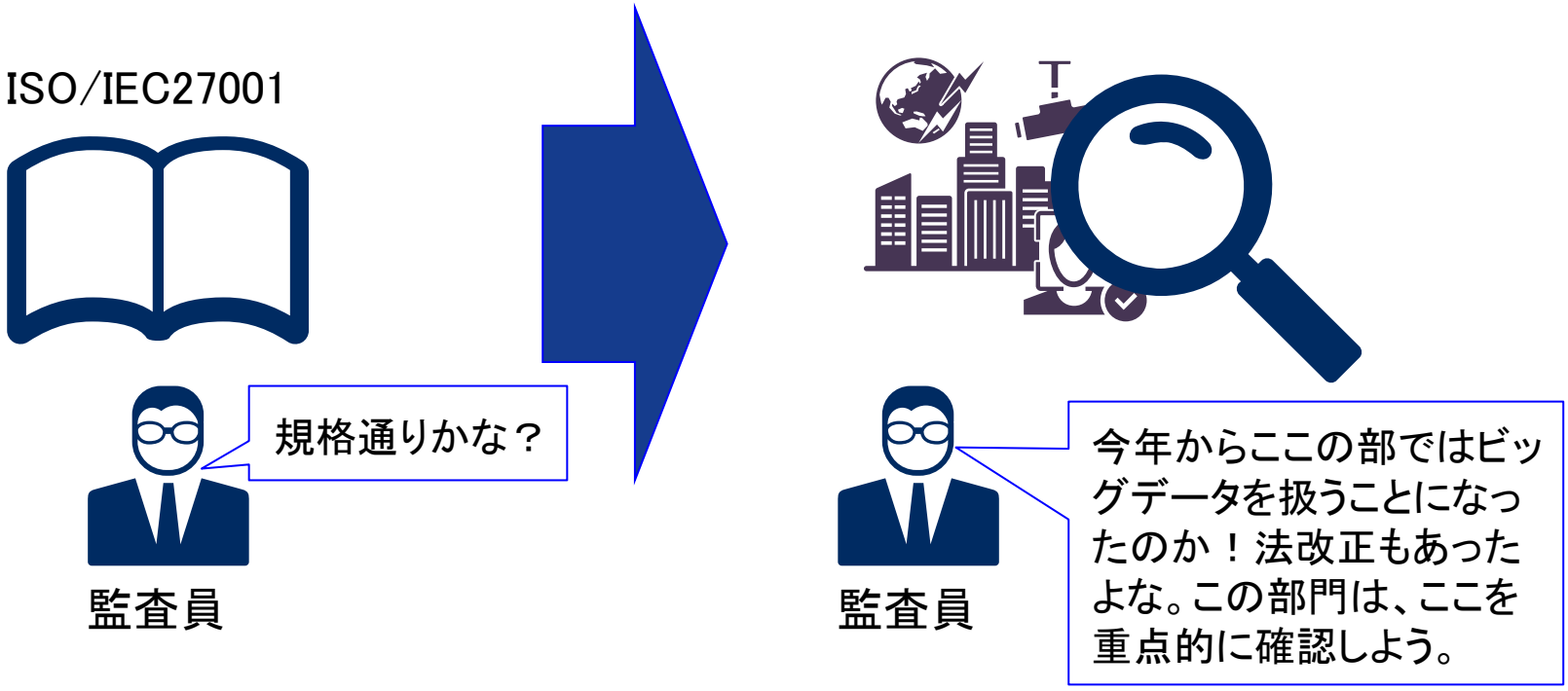

リスクを見逃すと



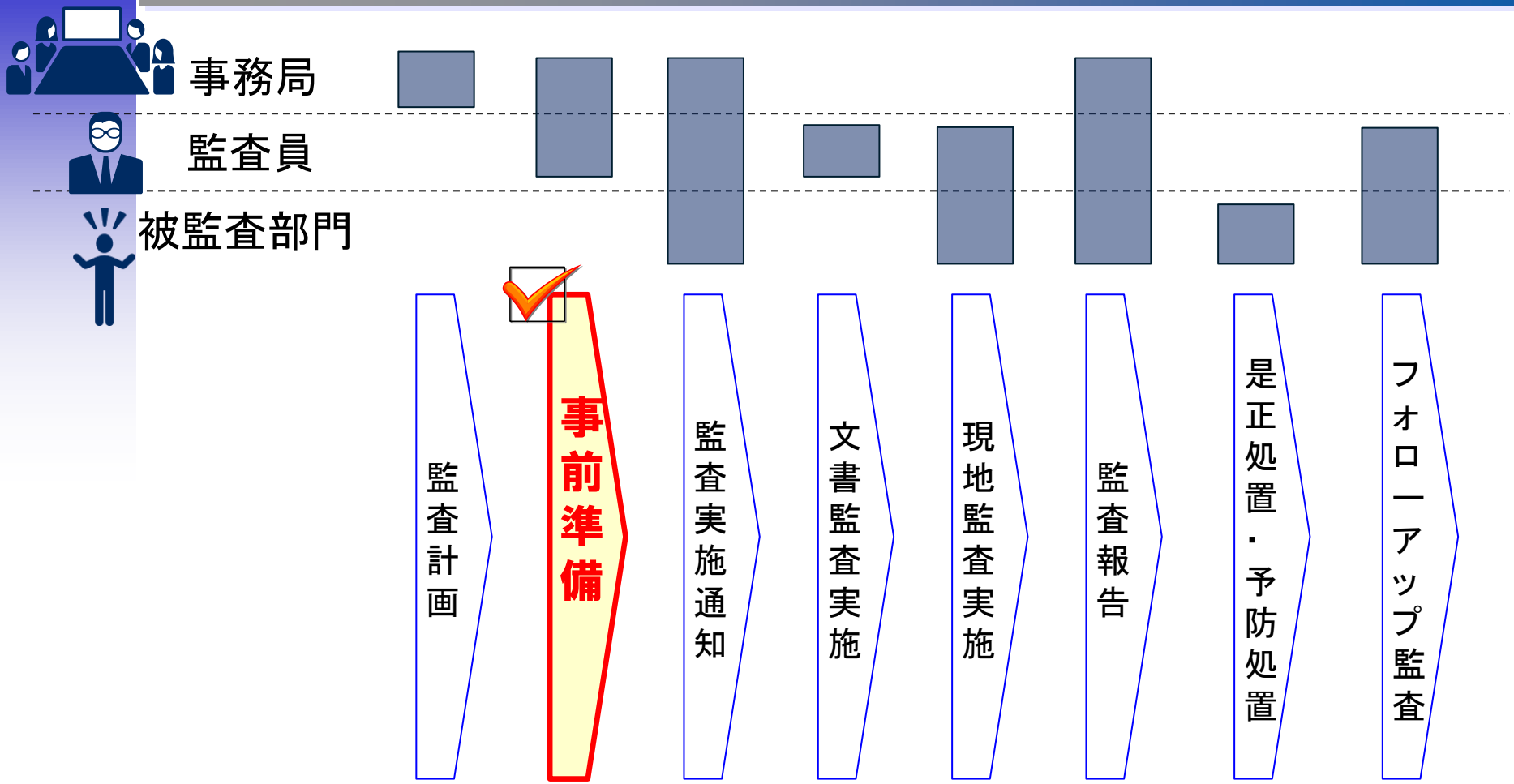
# 対策検討：
# 有効な監査の為の事前準備

# 有効な監査へ

皆さん、恐らくISMSの構築当初は、管理策114項目の適合性を内部監査で確認しているでしょう（適合性監査）。
組織の成熟に従い、内部監査は管理策114項目全てを網羅する監査から、リスクの高い管理策にフォーカスした監査にすべきである。管理策の導入目的の達成度合い、ISMSが有効・妥当かの有効な監査とすべきである。



# 監査の手順、どこが大事か




適合性監査の場合は、監査員は規格を理解していれば監査には支障がない。リスクにフォーカスした監査を意図する場合は、被監査部門の業務の理解が必要であり、業務を理解した上で監査に臨み、その組織のビジネスの維持･向上のための監査とすべく**事前準備がとても重要**となってくる。

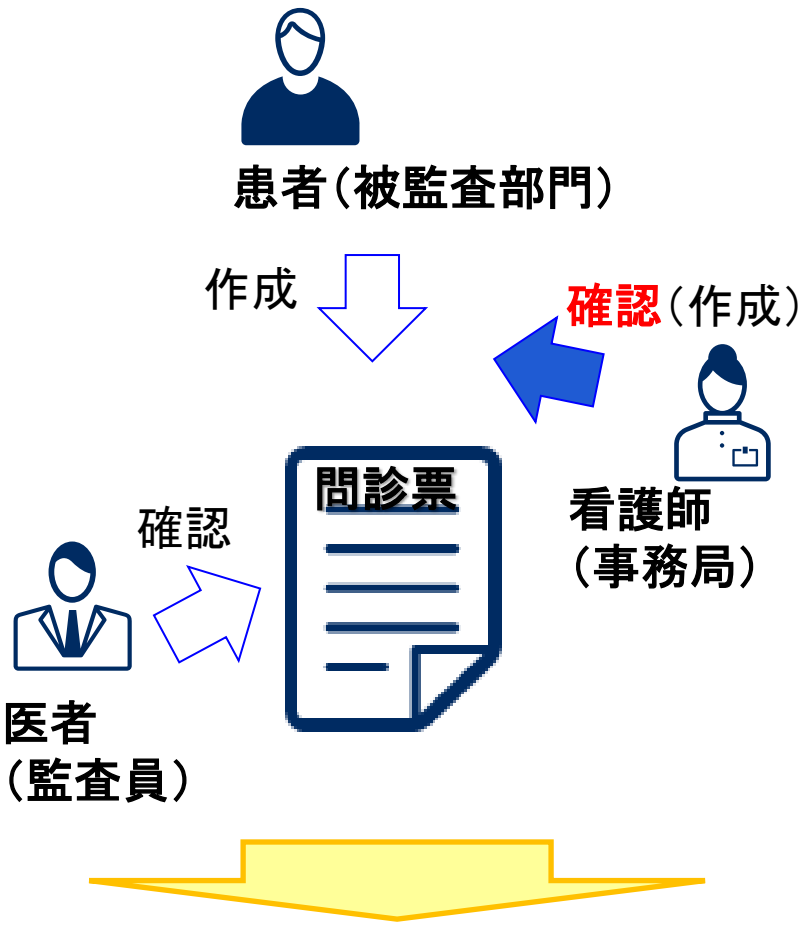
事前準備が大事！
それでは、内部監査をクリニックに例えて考えてみると・・
（クリニックでは、問診票をまず作成して診察しますよね）

# 問診票は、いつ、だれが作るか（クリニックに例えると．．１）

## 患者が作成


患者の誤記（投薬名の間違えなど）がありえ、正確性が低い

## 患者が作成したものを看護師が確認




患者の問診票は看護師が確認することで、誤記を防ぐ！

# 診察前にリスクを確認することで誤診を防ぐ（クリニックに例えると．．2）

医者

血圧は110で正常ですよ。お疲れなのですかね？頭痛薬を出しておきますね。それで、様子をみてください。

患者

先生、頭がとても痛いのです。見てください。

その後、救急搬送！
（残念なことに．．．．）

普通は、こんなこと無いですよね。

**問診票**

常用薬
・血圧降下剤

看護師

医者

血圧は110で正常だ！**問診をみると血圧降下剤を飲んでいる**のか。それで血圧は正常値なのか！

念のため頭のCTを取りましょう！

脳内の血管が破裂しそうです。緊急入院してください。

患者

先生、頭がとても痛いのです。見てください。

先生、頭痛の**原因を見つけてくれて有難うございました。大変なことになるところでした。**

**内部監査も患者（被監査部門）からこう言われる監査としたい！**

クリニックでは診察前の事前準備として「問診票」を有効に活用していました。
それでは、クリニックから内部監査に話を戻します。

# それではISMS内部監査はどうすべきか！

**要望**

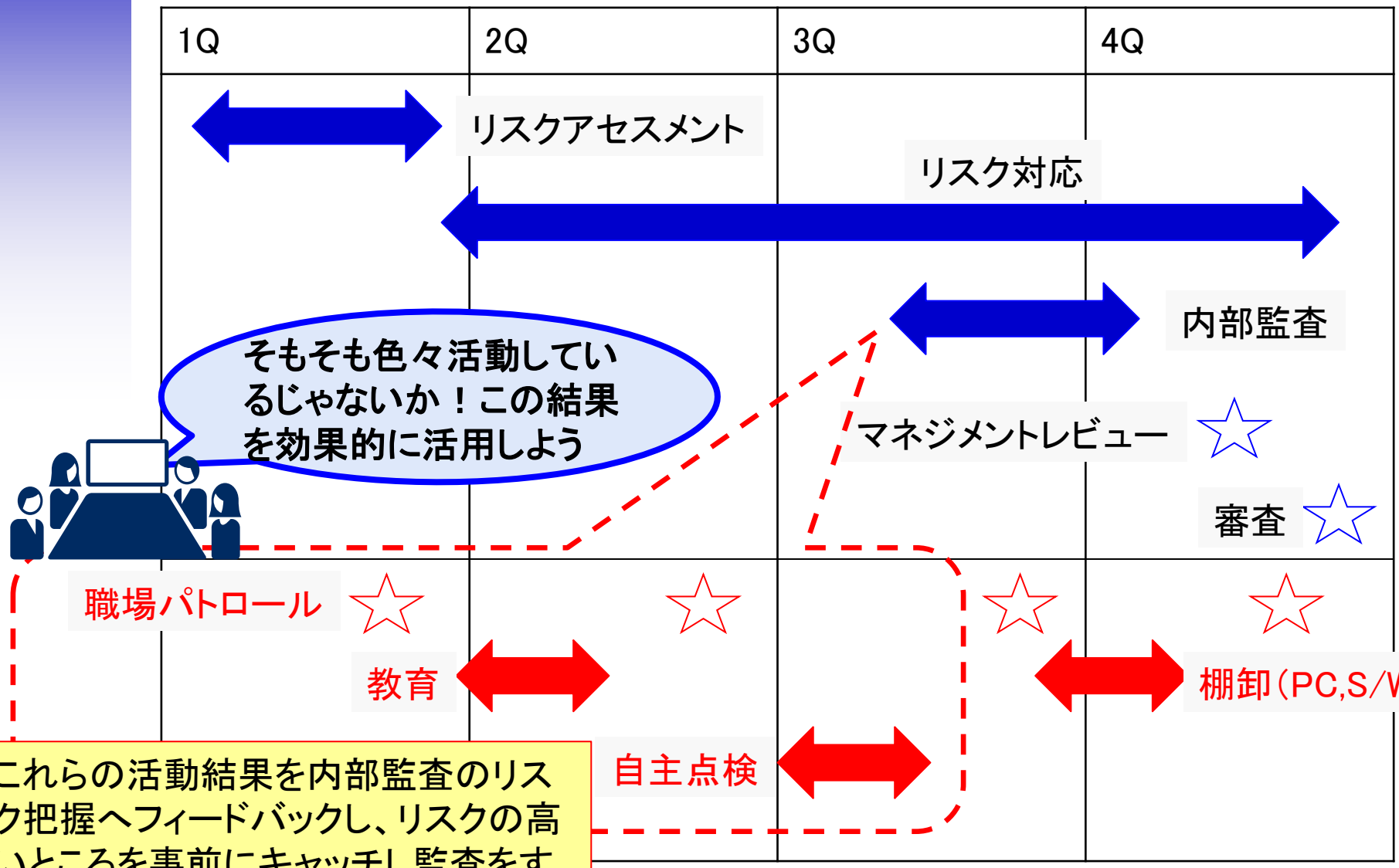
短い監査時間内で、組織のリスクにフォーカスして（リスクを見逃さないで）監査する必要がある

**対策**

情報セキュリティ施策は、年間を通していろいろと実施している。その施策の結果を活用したらどうだろうか！

**事前に、過去の活動結果（教育、自主点検、職場パトロール、審査、監査、インシデントなど）や日々の活動内容、業務の変化などを捉えて、当日の監査に臨めばよいのではないか！**

# 情報セキュリティ年間活動スケジュール（例）




これらの活動結果を内部監査のリスク把握へフィードバックし、リスクの高いところを事前にキャッチし監査をする。（**組織の事前情報を活用！**）

# 監査の事前準備作業の流れ

**被監査部門**
**（A開発部）**

**事前情報**

- 前回までの監査・審査結果
- 情報セキュリティインシデント
- 業務内容
- 人員構成
- PC台数
- ソフトウエア利用
- 年間活動結果（点検、教育、アンケート）
- ビジネス方針（キックオフ資料など）

A開発部の事前情報
（年間活動結果など）

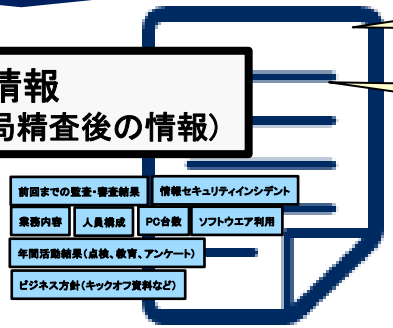
チェックシート(規格・社内ルールベース)を作成

**チェックシート**

- 規格
- 社内ルール

**事務局**

**事前情報**
**（事務局精査後の情報）**




事前情報収集

事前情報の精査を実施

- 持ち出し管理システム
- 出張精算システム
- 発注システム
- オーダー管理システム
- 構内作業者システム　等

**監査員**

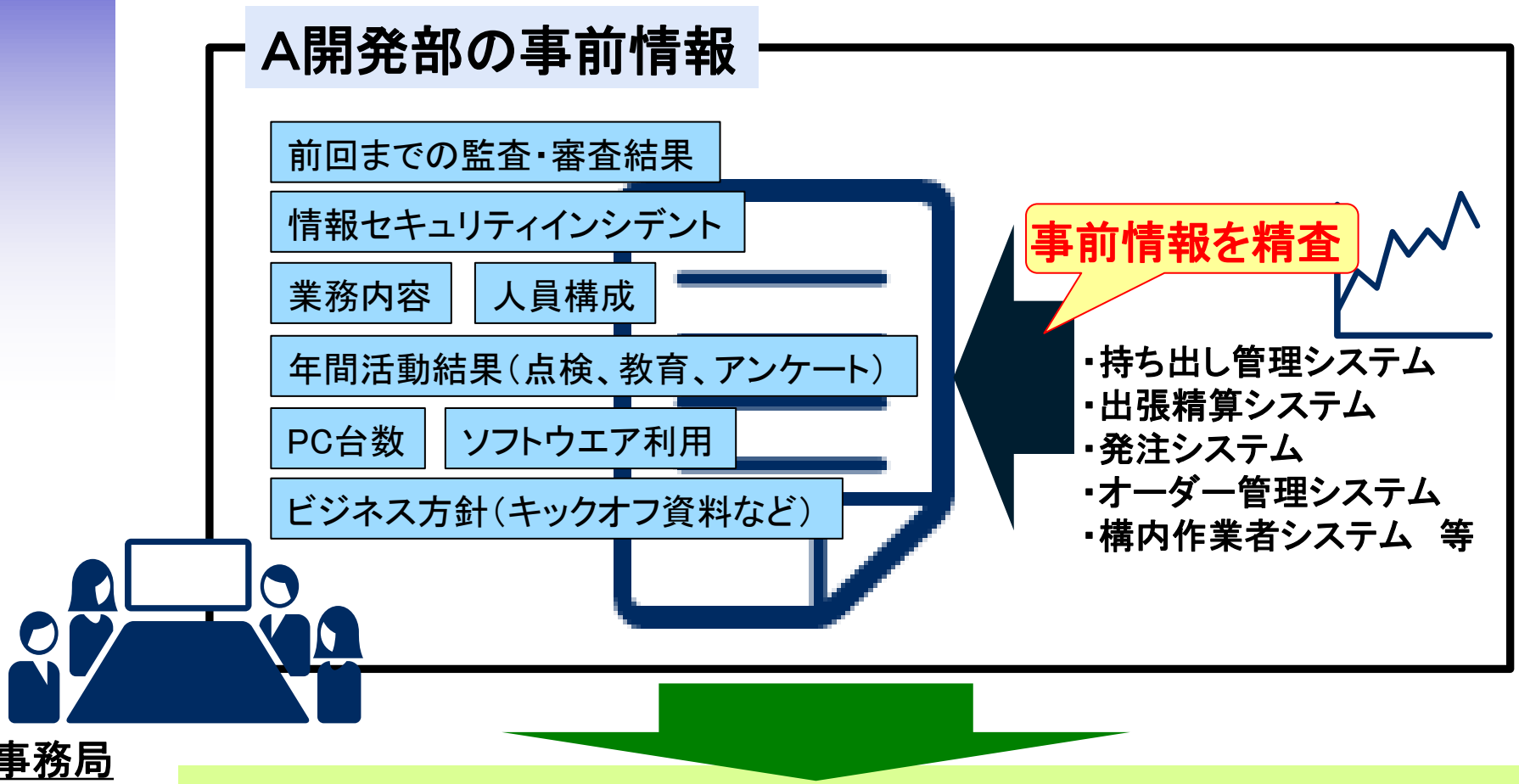
**監査項目抽出**

**チェックシートへ反映**

被監査部門の事前情報と事務局の精査した結果を基に重点監査項目を抽出し、チェックシートへ反映。

# 事前準備における情報を監査に活用しよう

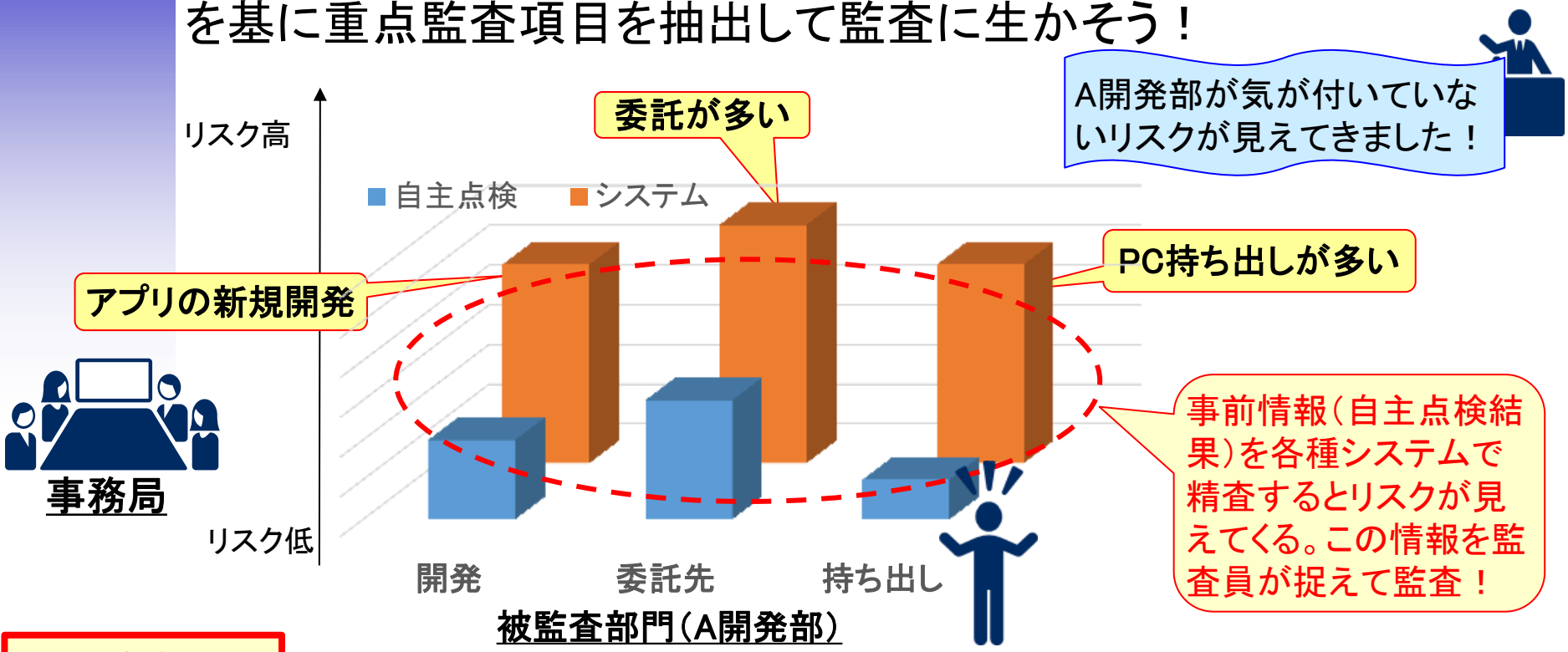
年間活動結果など事前情報を用意、それをシステムで精査！




本資料では、これを「**内部監査“問診票”**」と呼ぶこととした。（A開発部の各種活動をまとめたもの）

# 例：自主点検結果と実績データ比較からリスクが見えた！

年間活動の一例として「自主点検」の活用例を示す。自主点検結果を基に重点監査項目を抽出して監査に生かそう！




## 重点監査項目

各組織のリスクを事前に把握して、内部監査の項目を事前に整理！

監査員

| 【リスク】 | 【重点監査の視点】 |
|---|---|
| PCの持ち出し | 持ち出し管理のセキュリティ対策状況 ⇒ A.11.2.5資産の移動 |
| アプリの新規開発 | 開発におけるセキュリティ対策状況（アプリの脆弱性確認など） ⇒ A.14.2開発のセキュリティ |
| 委託が多い | 委託先のセキュリテイ対策状況（秘密保持契約など） ⇒ A.15供給者関係 |

# 従来のチェックシートと問診票活用の違い

## チェックシート(網羅的)


| | | | |
|---|---|---|---|
| A.5 方針 | A.6 内部組織 | | A.8 資産の管理 |
| A.9 アクセス制御 | A.10 暗号 | A.11.1 物理的セキュリティ | A.11.2 装置の管理 |
| A.12.2 マルウエアからの保護 | A.12.6 技術的脆弱性管理 | A.13 通信のセキュリティ | A.14.2 開発のセキュリティ |
| A.15 委託先管理 | A.16 インシデント管理 | A.17 事業継続 | A.18.1 法・契約の順守 |

点検項目一つずつ網羅的に確認

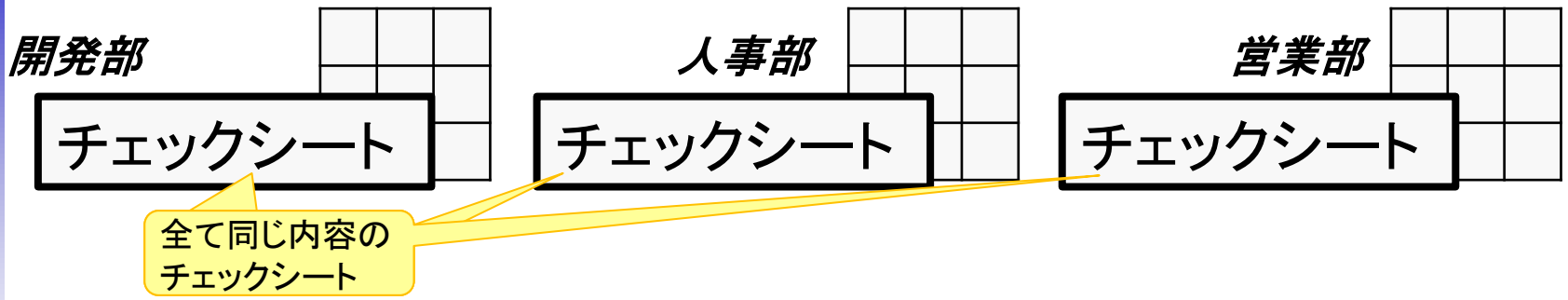
## 重点リスクを反映したチェックシート


| | | | |
|---|---|---|---|
| A.5 方針 | A.6 内部組織 | | A.8 資産の管理 |
| A.9 アクセス制御 | A.10 暗号 | A.11.1 物理 | A.11.2 装置の管理 |
| A.12.2 マルウエアからの保護 | A.12.6 技術的脆弱性管理 | A.13 通信のセキュリティ | A.14.2 開発のセキュリティ |
| A.15 委託先管理 | A.16 インシデント管理 | A.17 事業継続 | A.18.1 法・契約の順守 |

関連するこれらの運用状況も確認！

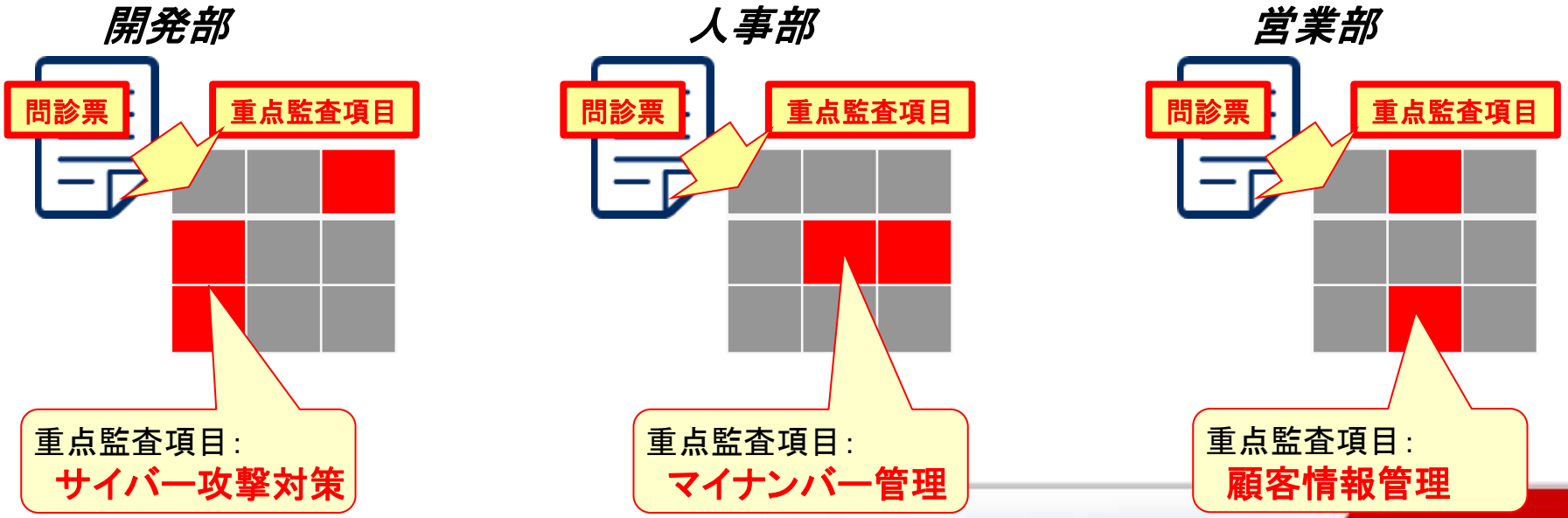
A.11.2
A.14.2
A.15に
フォーカス
して監査！

# 従来のチェックシートとの違い(事前に組織のリスクをキャッチ)




同じチェックシートでは、監査漏れ
(その部固有のリスクの確認漏れ)
が起きる可能性がある

## 重点リスクを反映した“チェックシート”

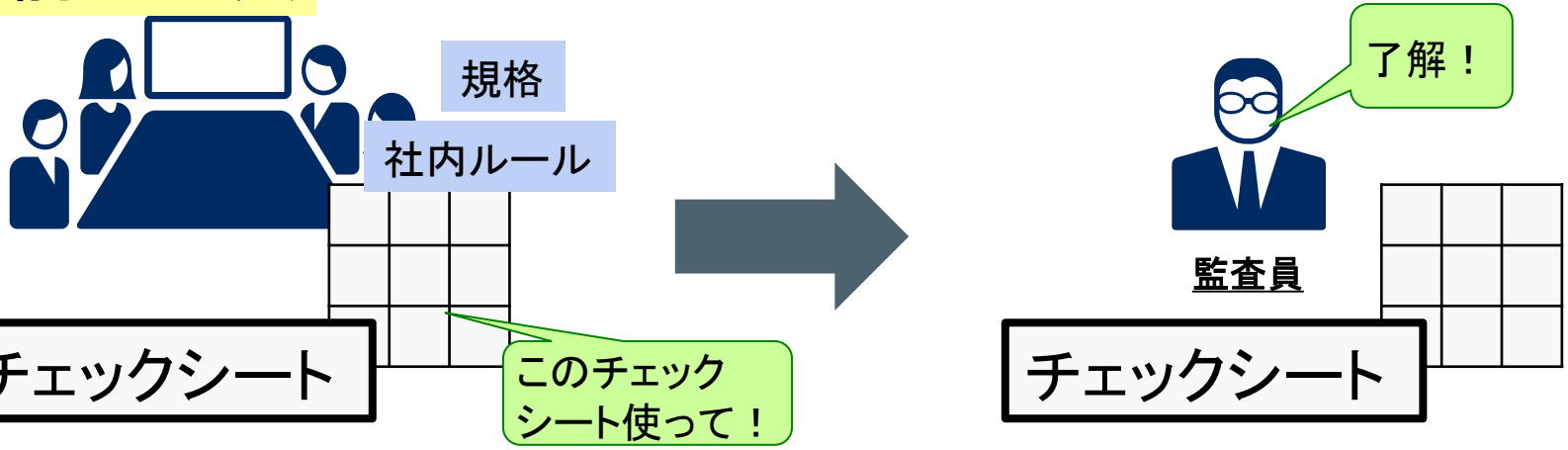


このように、日々の活動結果を基にして、部門固有のリスクを事前に把握して、監査に臨むことができるのです！

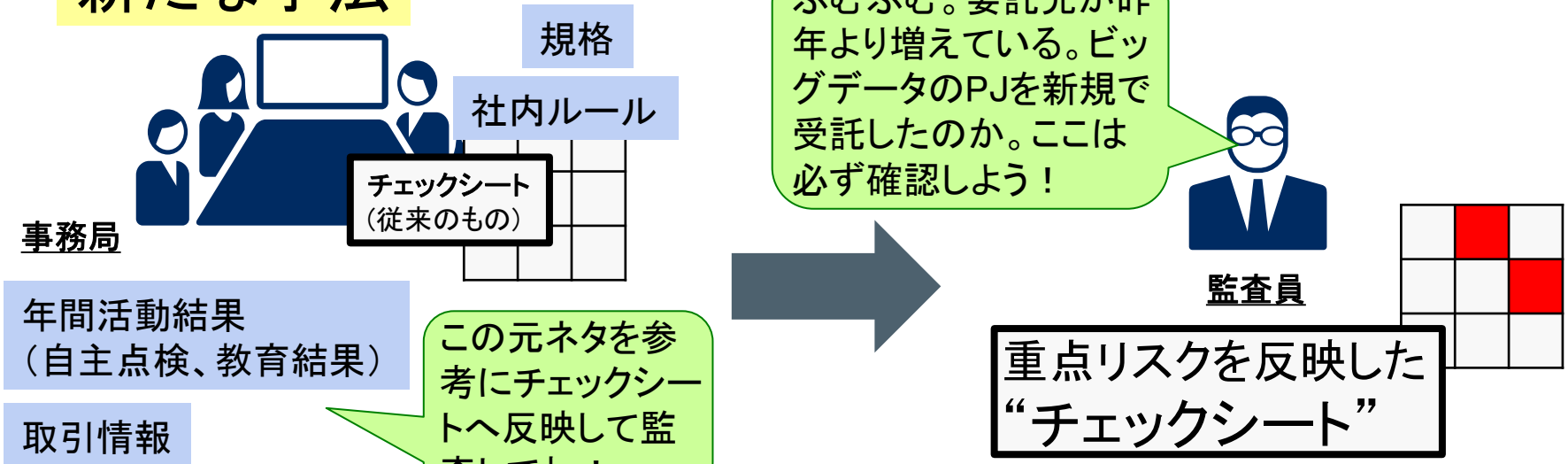
従前の監査手法と異なり、更に監査員へのメリットもあるのです。

# 従来の内部監査の事前準備との違い

## 従前の手法




## 新たな手法



# 問診票活用・運用のメリット

問診票で．．．
- 各部固有の情報を事前に確認
- 監査員が重点監査項目を確認

リスク（変化点等）を把握

監査員が重点項目をチェックシートへ反映

**重要なリスクの監査漏れ（忘れ）を防ぐ**

**監査員の育成・力量向上**

# 実際に「問診票」を導入した組織での声

被監査部門

効果：

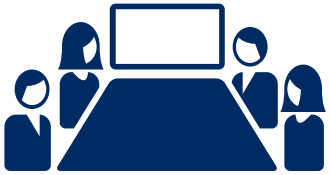
監査時間は短いが、的を得た監査で良かったとの現場の声があった。限られた監査時間を有効に活用できた。

被監査部門からの意見の一部：**“監査のために事前に準備してきたんだね..。今回はとんちんかんな監査でなかったね..”**

【導入した経緯】

監査が毎年組織共通の重点監査項目に全部門がフォーカスしてしまい。本当にリスクのあるところにフォーカスした監査ができていなかったために導入した。**各組織の業務内容やリスク、特徴に応じ、濃淡つけた監査ができていなかった。**（監査時にヒアリングして状況収集して監査するとなると、時間も要すし、本当に見なければならないところに時間をかけれなかった）

事務局



次のページでは、問診票の更なる活用を示します。

# 問診票の応用 （問診票 ⇒ 監査結果 ⇒ 監査カルテ）

監査結果（監査報告書）とその是正処置を積み上げた「監査カルテ（仮名）」を作成する（データベースのイメージ）。

【メリット】

**被監査部門**：「監査カルテ」は組織のセキュリティガバナンスの記録(不適合と是正の記録)であり、**組織の経年変化を正しく把握**することが可能。

**監査員**：「監査カルテ」から、類似な業務形態の組織を見て**リスクを予想して監査**に臨むことが可能。

**事務局**：組織の多岐に渡る累積した活動を「監査カルテ」としてデータベース化することで、**事務局メンバの交代時**に大きな引継ぎ作業を要せず対応可能。

# 例：問診票の応用

A開発部

2017年度

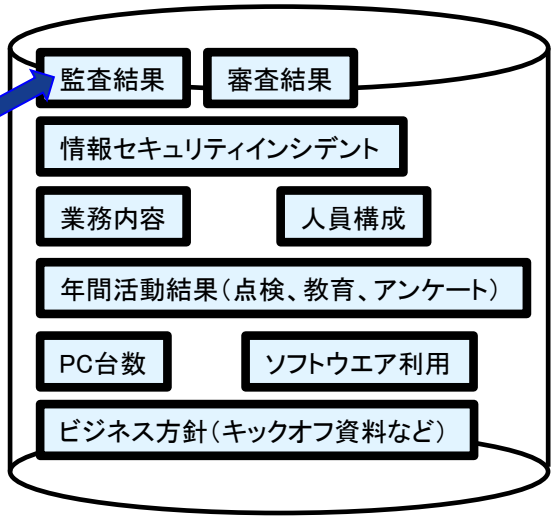
問診票

重点監査項目

重点リスクを反映したチェックシート

内部監査

監査結果




**A開発部　監査カルテ**

2018年度

問診票

重点監査項目

重点リスクを反映したチェックシート

内部監査　・・・・

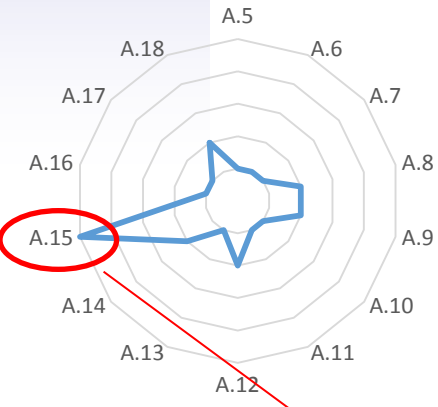
毎年の監査結果、その他の年間活動結果を積み重ねてセキュリティに関わる経年変化をまとめる（本書ではこれを“**監査カルテ**”と呼ぶ）。“監査カルテ”は、次年度の問診票のベースともなる。

# カルテの活用：その不適合は慢性疾患か急性疾患なのか

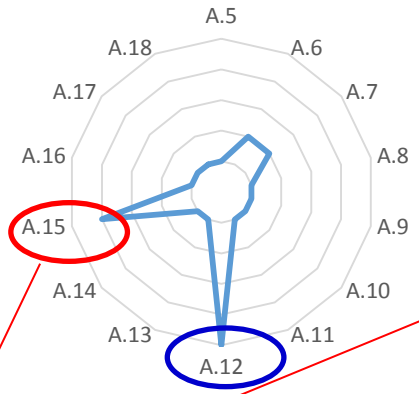
内部監査記録の経年変化を記録することで、その不適合が慢性的に起きているのか突発的な事象だったのか確認することができる。
慢性的な場合は、是正処置が機能していないと考えられ、新たな目線での内部監査計画を立案する必要がある

図の見かた：外側ほどリスクが高い（不適合が多い）

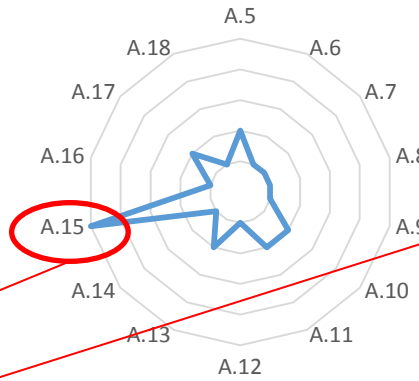
2013年度



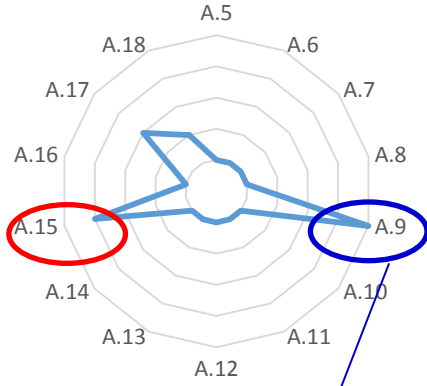

2014年度



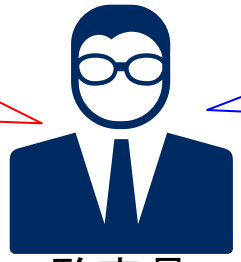

2015年度




2016年度




A.15（委託先管理）が毎年の監査結果で不適合とされている。内部監査では重点的に確認をしなければ！**ルールがおかしいのかもしれない。監査計画を再考**しよう。



監査員

2017年度の監査はどこを見よう？うむ、A.9項で不適合があるぞ。開発サーバの**利用者が増えてきた（変化点）**ことによるアクセス制御にリスクがあるようだ。

# まとめ

- 問診票を事前に用意することで1年に一度の内部監査を有効に運用
- チェックシート作成など重点監査項目を検討させることは、内部監査員の育成につながる
- カルテとして監査結果を積み上げていくことで組織の経年変化を確認することが可能、それを踏まえて今後の監査に生かすことも可能
- カルテを活用することで、事務局メンバ交代時にスムーズにメンバ移行も可能

# さいごに

**是非とも、本研究会へ参加いただき、実際の議論の場を体験し、自組織の課題解決に繋げて頂ければと思います。**

〔連絡先〕
**日本ISMSユーザグループ事務局**
NTTデータ先端技術株式会社
〒104-0052　東京都中央区月島1-15-7
パシフィックマークス月島
e-mail　：　info@j-isms.jp
URL　　：　http://j-isms.jp/index.html