サイバーセキュリティの監査

1月29日

特定非営利活動法人日本セキュリティ監査協会
エグゼクティブフェロー
永宮直史

CONTENTS

自己紹介

- 永宮　直史　（ながみやただし）
  - 特定非営利活動法人　日本セキュリティ監査協会　エグゼクティブフェロー
  - 公認情報セキュリティ主席監査人
  - 委員等
    - 政府機関におけるクラウドサービスの安全性評価に関する検討会委員
    - 産業サイバーセキュリティ研究会WG1第３層TF　構成員
    - エネルギー・リソース・アグリゲーション・ビジネス検討会サーバーセキュリティWG委員
    - ISO/IEC JTC1 SC27 WG1及びWG4国内委員
    - クラウドセキュリティコントロール標準化専門委員会委員（2016年度まで）
    - IoTセキュリティガイドライン SC 27/WG 4対応 小委員会委員
  - 2015年　情報セキュリティ文化賞受賞、2019年　標準化貢献賞受賞
  - 略歴
    - 1973年野村総合研究所入社；公共政策立案等のコンサルティング
    - 1996年インターネット事業関連部署の事業企画室長（セキュリティ事業立上）
    - 1999-2002年ソウル支店長（地域計画、インターネット事業調査）
    - 2002-2006年日米合弁のセキュリティベンチャー企業CTO、CSO
    - 2006-2011年金融持ち株会社情報セキュリティ事務局
    - 2011-2019年8月　日本セキュリティ監査協会事務局長
    - 2019年9月-　現職

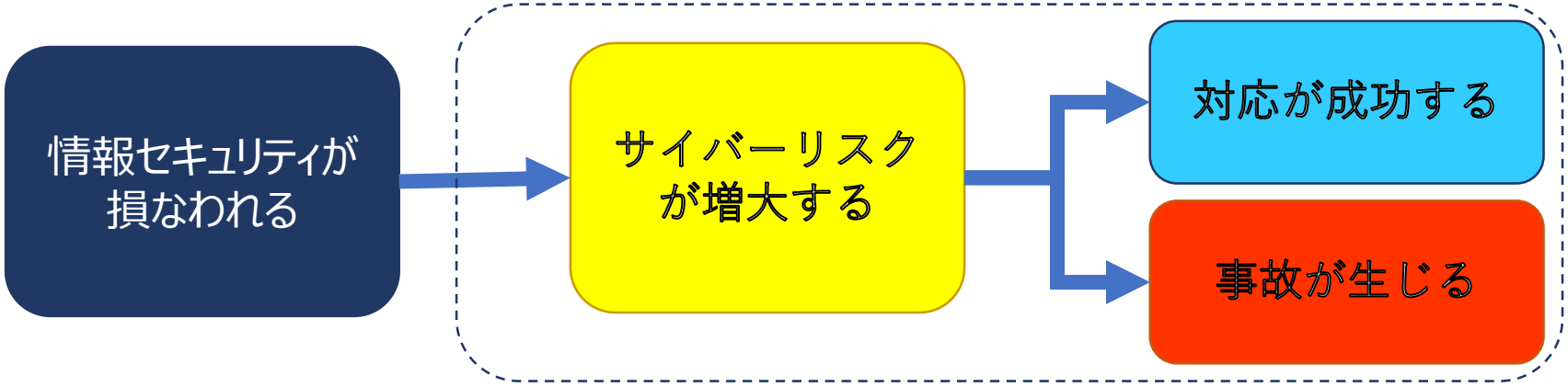
1.情報セキュリティとサイバーセキュリティ

2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

概念の比較

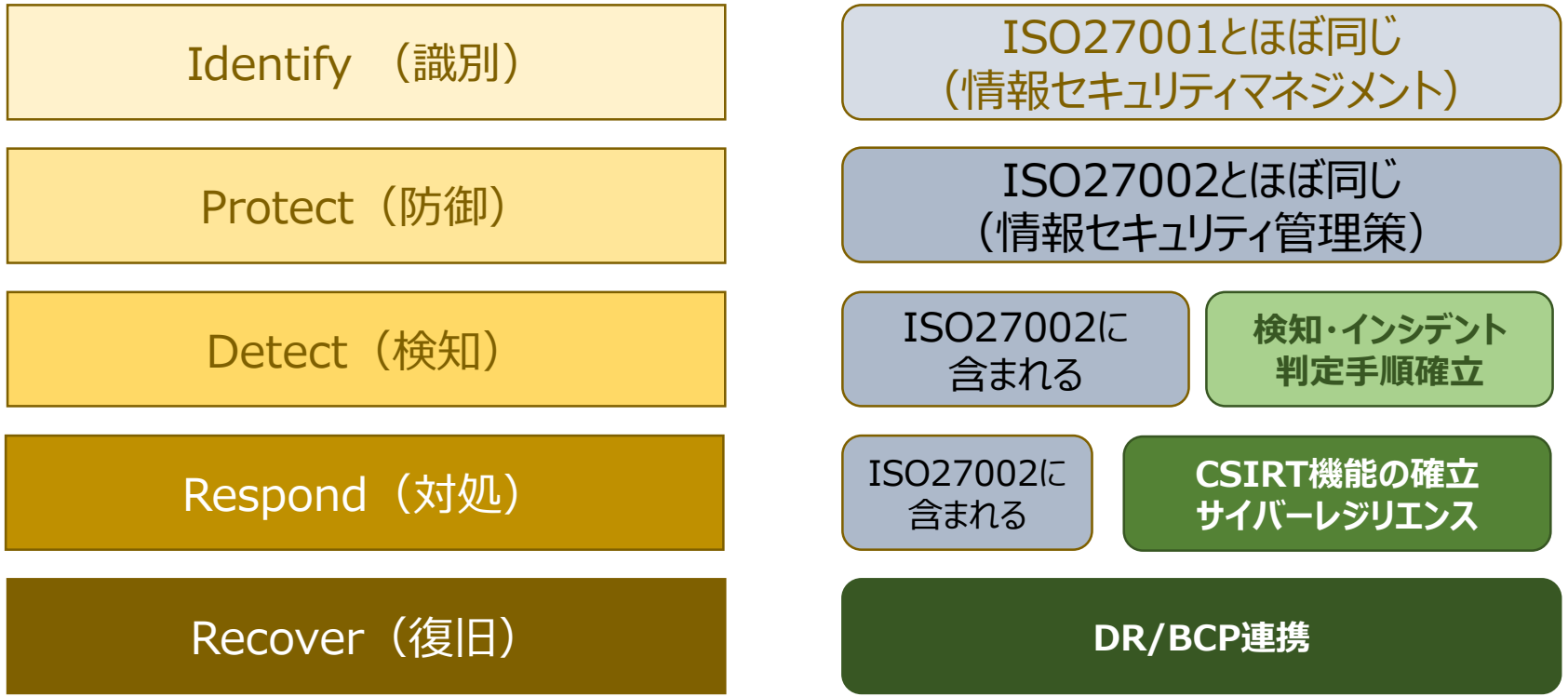
	情報セキュリティ	サイバーセキュリティ
定義	機密性・完全性・可用性を守ること	サイバーリスクから人・組織・社会の安全を保つこと
範囲	情報（デジタル、アナログ、物理媒体）	サイバー空間
リスク	情報の棄損	人的・物的損害

※サイバーリスク：サイバー空間における脅威がもたらすリスク
サイバー空間：ネットワーク、サービス、システム及びプロセスにより相互接続されたデジタル空間
事件事故の対処は既存のフィジカルな対応で行う



【情報セキュリティ】　【サイバーセキュリティ】

サイバーセキュリティとISMS



（サイバーセキュリティフレームワーク）　　（ISMS）

サイバーセキュリティの要点

要点１

リスク評価

- ■ 人的・物的被害に着目したリスク評価
  - □ ISO31000に基づくリスク評価を追加
    - ✓ めったに生じないが、甚大な被害が生じるリスク（想定外を想定する）

要点2

情報セキュリティ防御ができなかった場合の対策を強化

- ■ 検知手順・インシデント判定手順の確立
- ■ CSIRTの確立
- ■ 事業継続：物理的対処チームや復旧プロセス等との連携及びサイバーレジリエンスの確立

※サイバーレジリエンス：
損害を被ったシステム部分を除いて、業務を継続する仕組みがあること

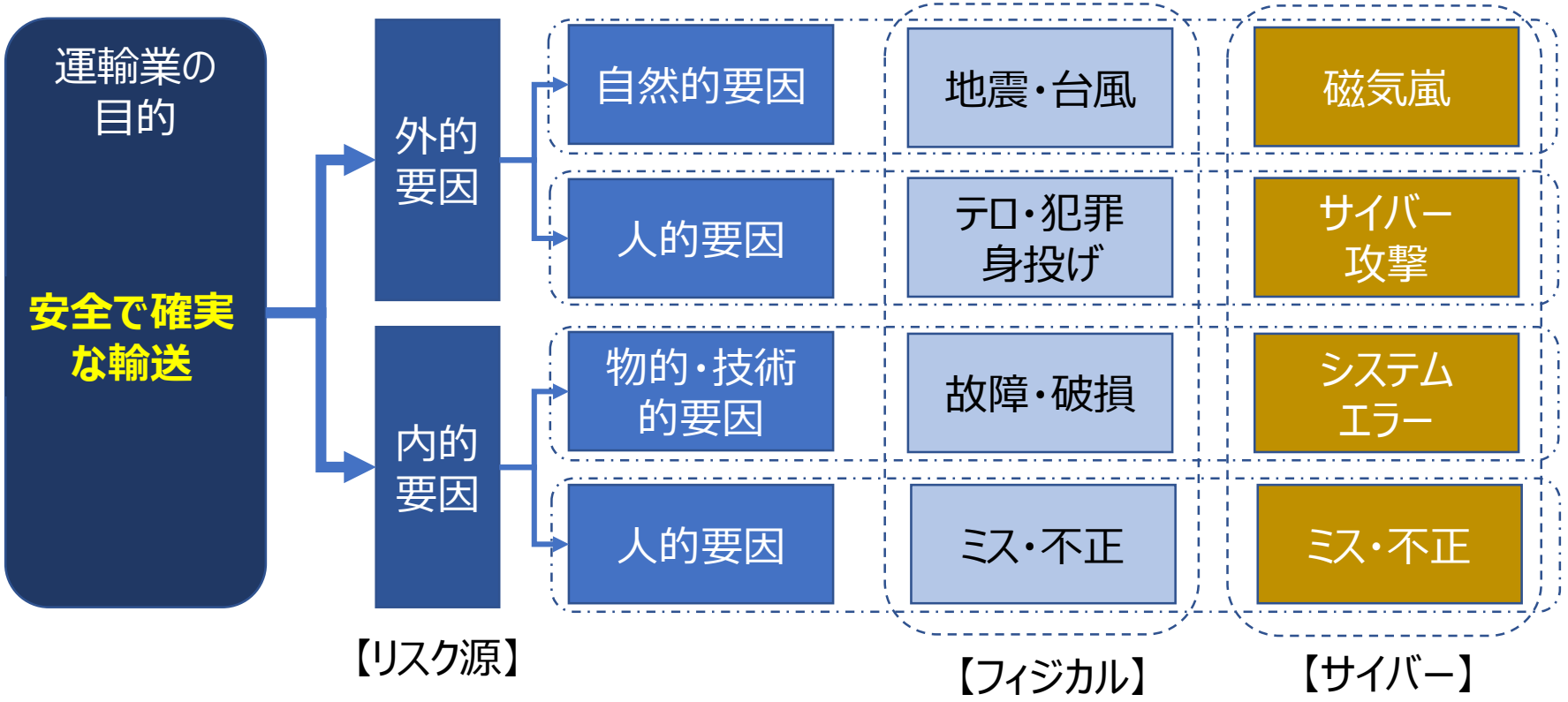
2.サイバーセキュリティのリスク判断

1. 情報セキュリティとサイバーセキュリティ

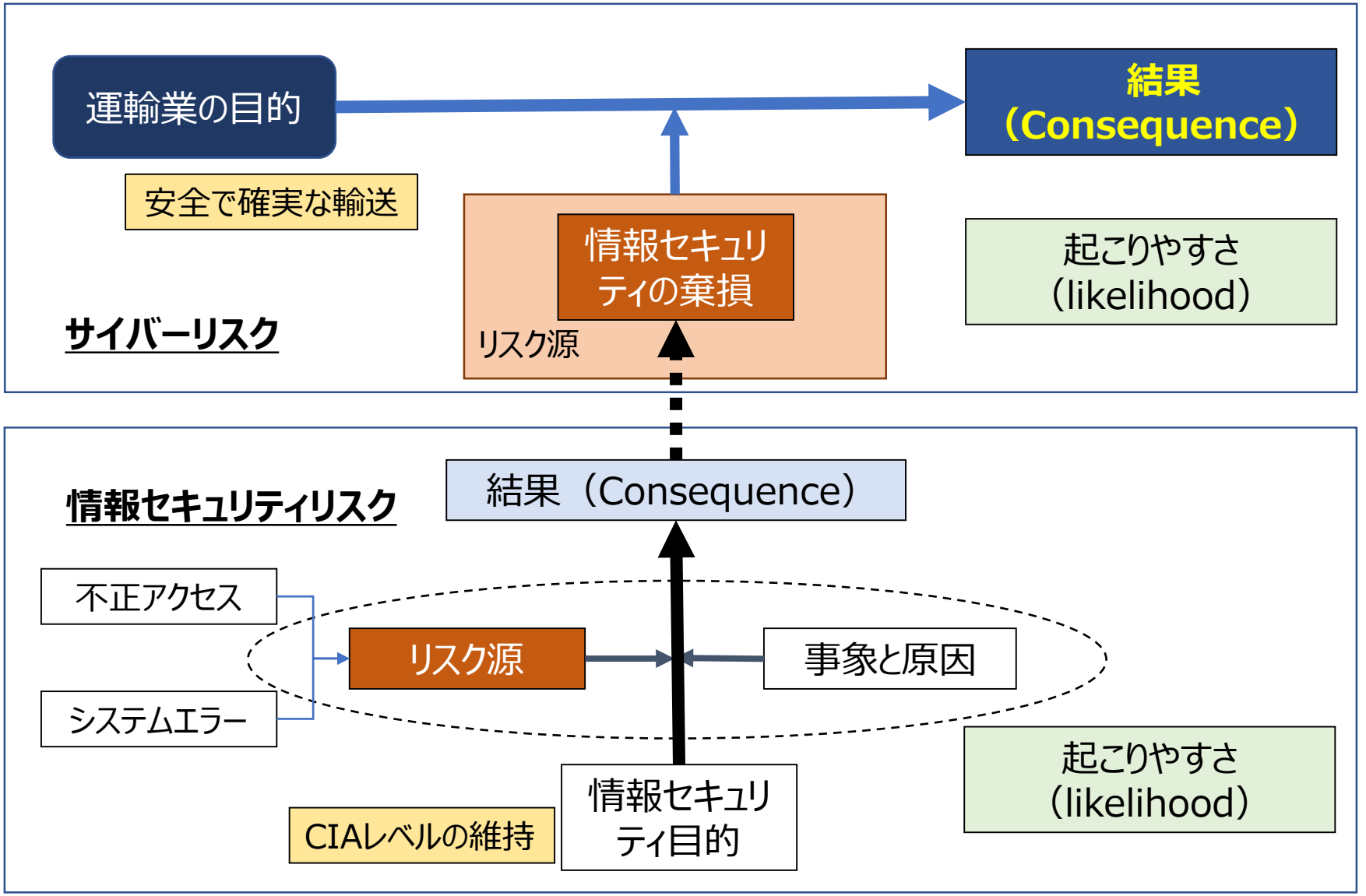
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

リスクとは

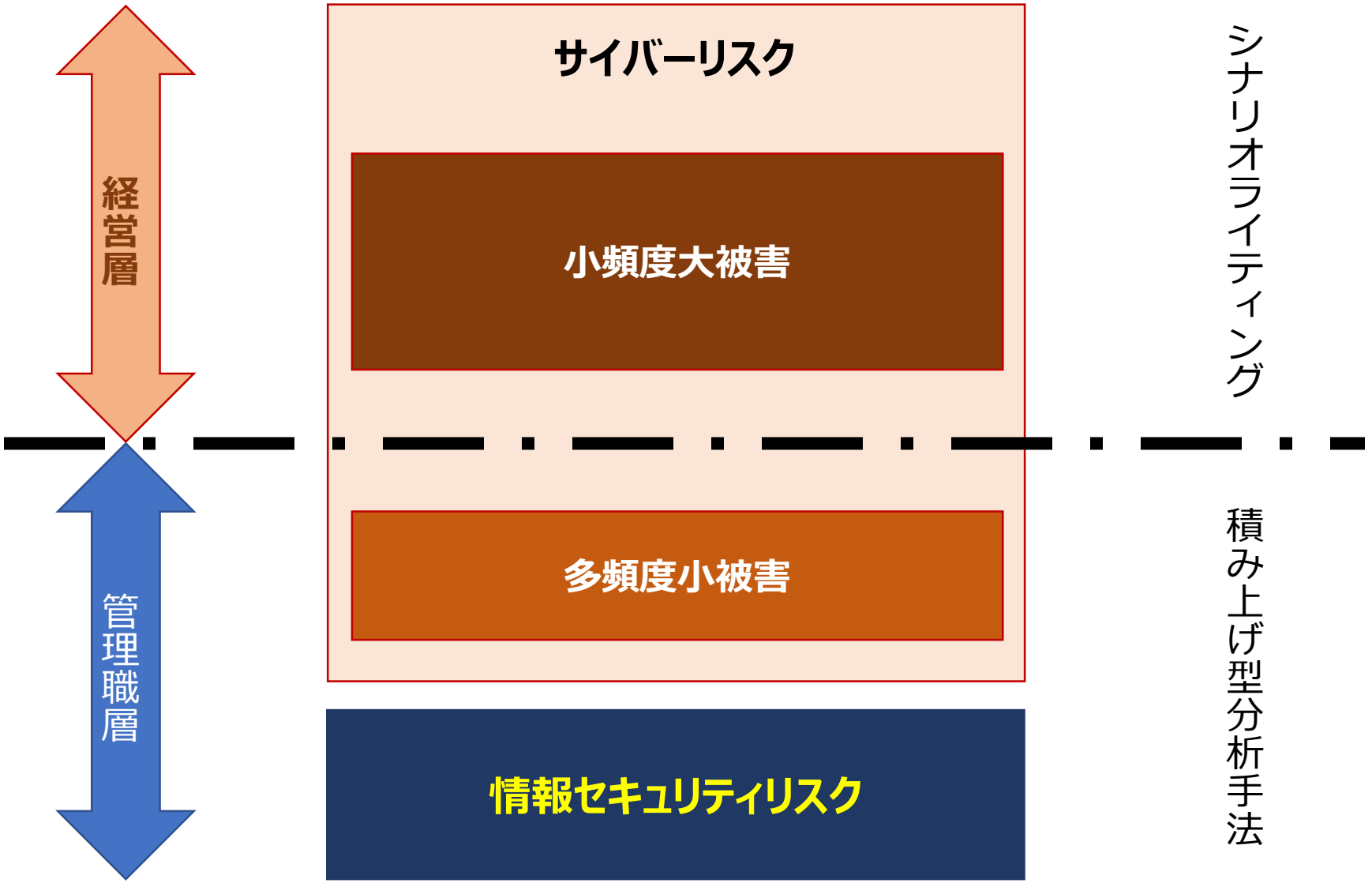
リスク：目的に対する不確かさの影響
（ISO31000）



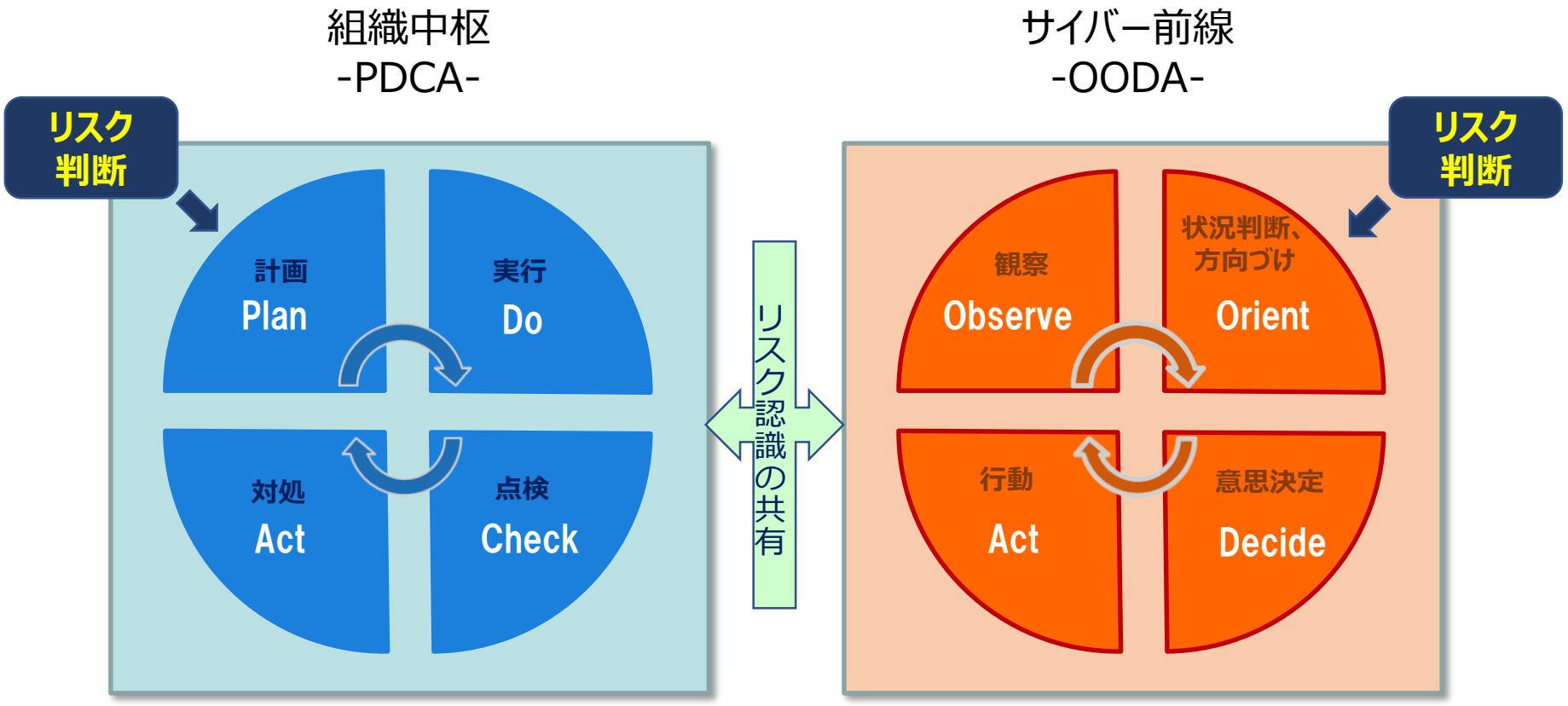
情報セキュリティリスクとサイバーリスク



サイバーリスク判断における経営の役割



二つの活動とリスク判断



組織戦略としてのリスク判断
長いサイクル（1年間など）

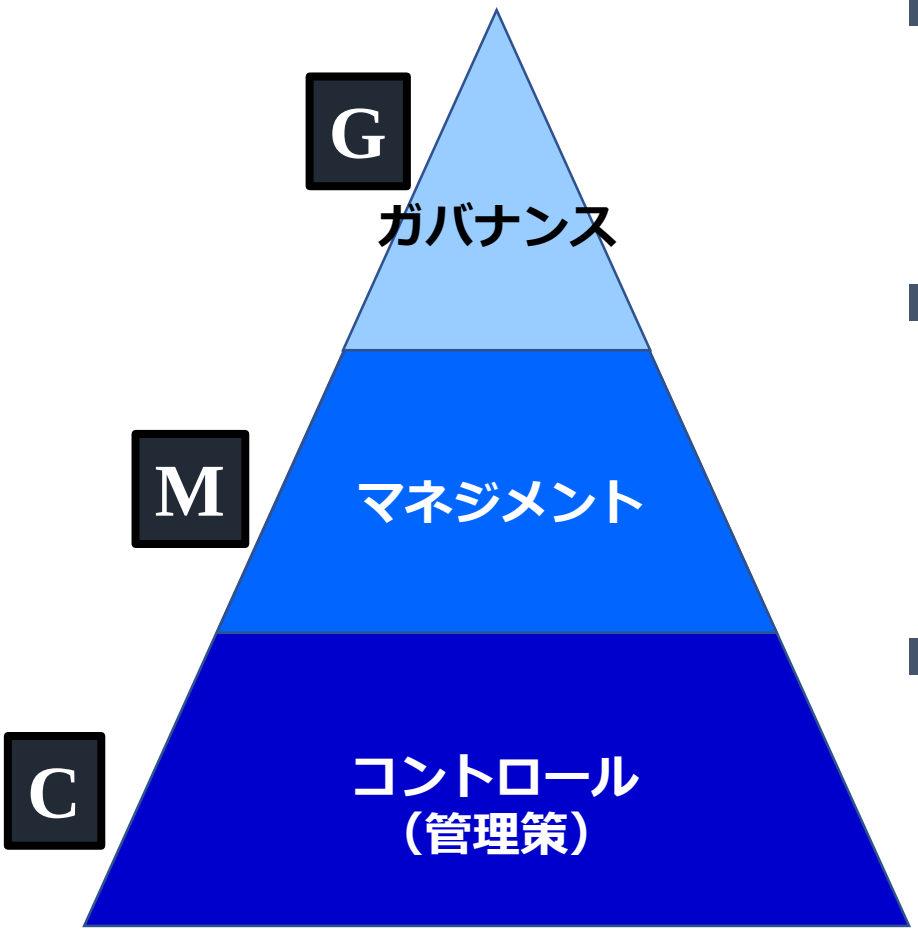
事故回避のためのリスク判断
短いサイクル（数時間～数日）

3. ガバナンス・マネジメント・コントロール

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断

4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

GMC



■ガバナンス

- 経営が企業全体としての意思を明確にし、それを貫徹する

■マネジメント

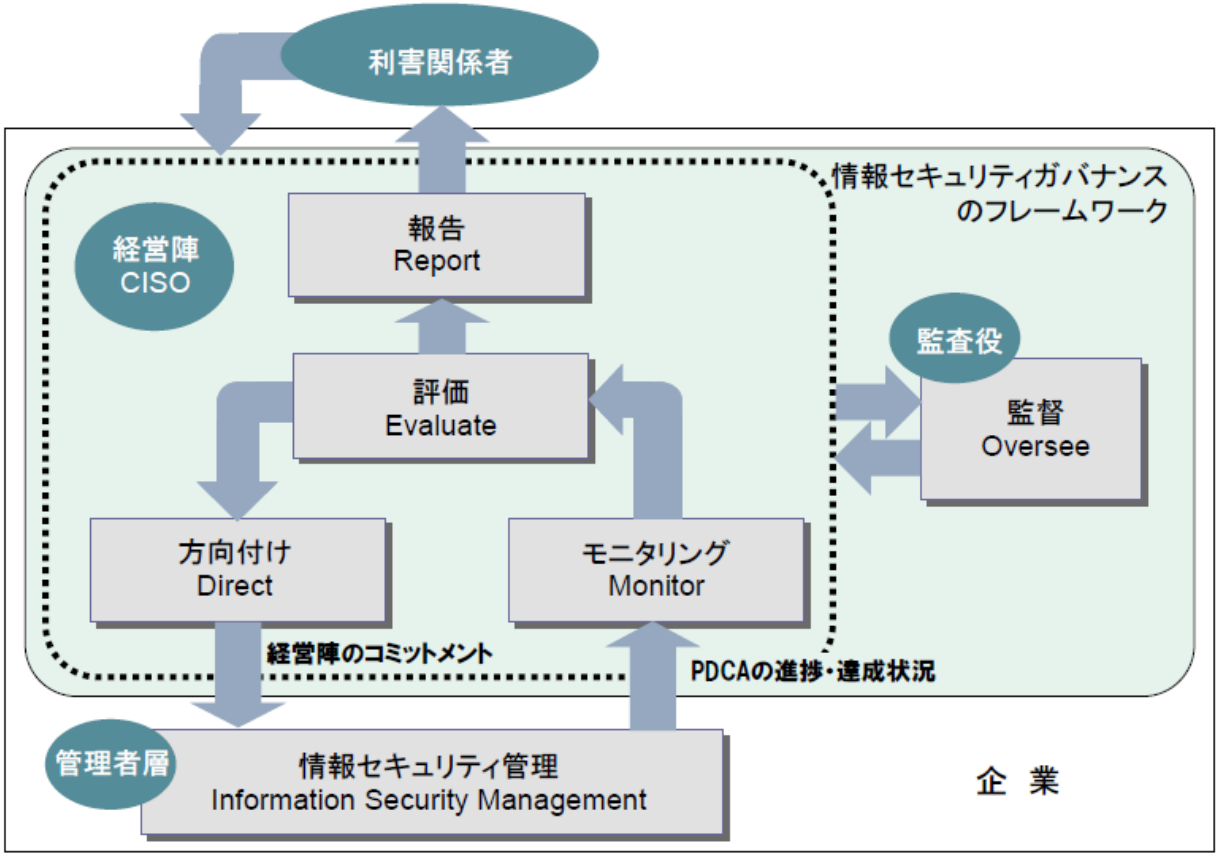
- 管理職が管掌する範囲で経営の意思を反映した成果をだすようにする

■コントロール

- 担当者が定められたことに従って行動する

セキュリティガバナンスの構造

情報セキュリティガバナンスのフレームワークはサイバーセキュリティガバナンスにも適用できる



- 方向づけ（Direct）
- モニタリング（Monitor）
- 評価（Evaluate）
- 報告（Report）
- 監督（Oversee）

「情報セキュリティガバナンス導入ガイダンス」

重要なリスクコミュニケーション

組織全体でリスク認識が共有されていると、ガバナンスが利きやすい

■リスクコミュニケーション※の意義：

- 組織内外の関係者が「リスク」「意思決定の根拠」「特定の活動が必要な理由」についての理解が容易になる

■リスクコミュニケーションの実施段階

- リスクアセスメントのみではなく、リスク対策の実施、レビュー、記録等リスクマネジメントのあらゆるプロセスで行う
- サイバーセキュリティ対策もリスクマネジメントプロセスとして行われる

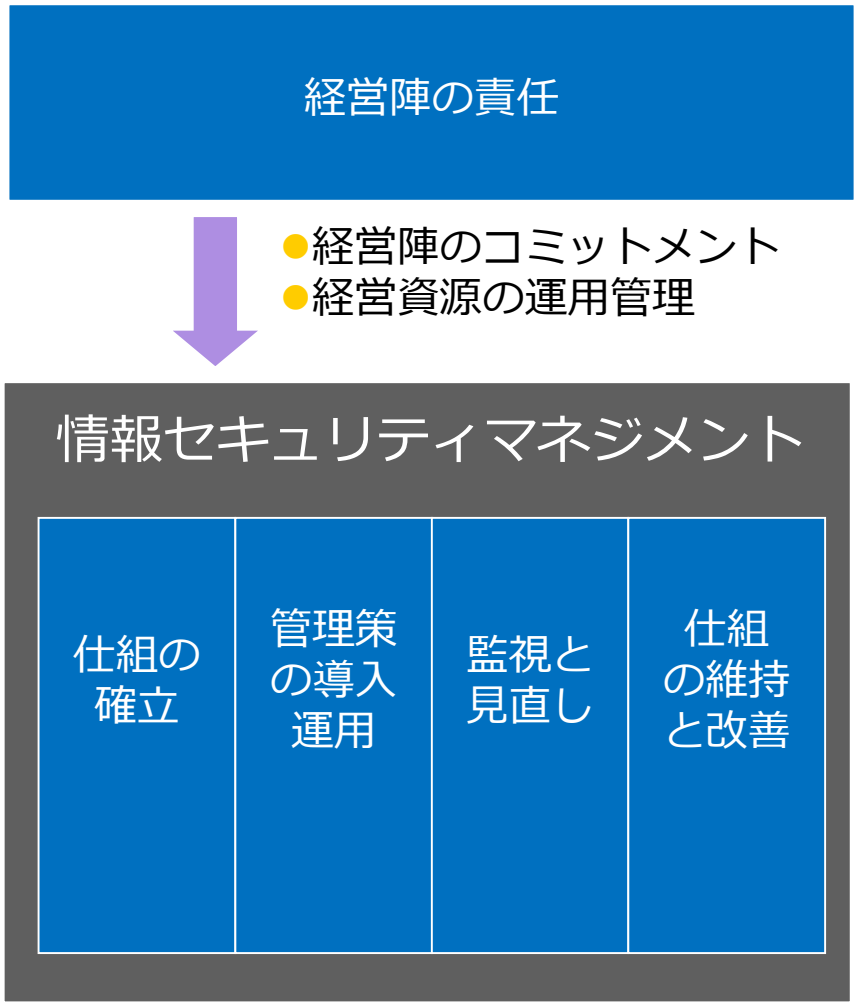
■リスクコミュニケーションのねらい

- プロセスの各段階で組織内外の専門家の知識を集める
- リスク基準を定め、リスク評価の場合に異なる見解に考慮する
- リスク監視及び意思決定を行うための十分な情報を提供する
- **リスクの影響を受ける者たちの一体感と当事者意識を醸成する**

（注）ISO31000：2018に基づき加工

※　ISO31000では「リスクコミュニケーション及び協議」

セキュリティマネジメントシステム



a. 基本方針を確立する
b. 目的を定め、計画の策定を指示する
c. 情報セキュリティに対する役割や責任を定める
d. 情報セキュリティの重要性を組織内に周知する
e. 必要な経営資源を提供する
f. リスク受容の基準、受容可能なリスクの水準を決める
g. 内部監査の実施を指示し支援する
h. 経営者の視点からレビューを実施する

（ISO/IEC27001：2005による）

4.基本となる情報セキュリティ監査

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール

5. サイバーセキュリティの監査
6. 監査役の役割

監査とISMS

- 監査の目的
  - 情報セキュリティマネジメントが効果的か
- 監査の方法
  - 準拠性監査
    - 組織が定めたルールに準拠しているか
  - 有効性（妥当性）監査
    - リスク管理が有効か（管理策がリスクに対して妥当か）

⇒ 有効性監査が必要

- ISMS適合性評価制度の限界
  - 監査の方法等は経営者が決める
  - ISO27006により審査工数の上限がある

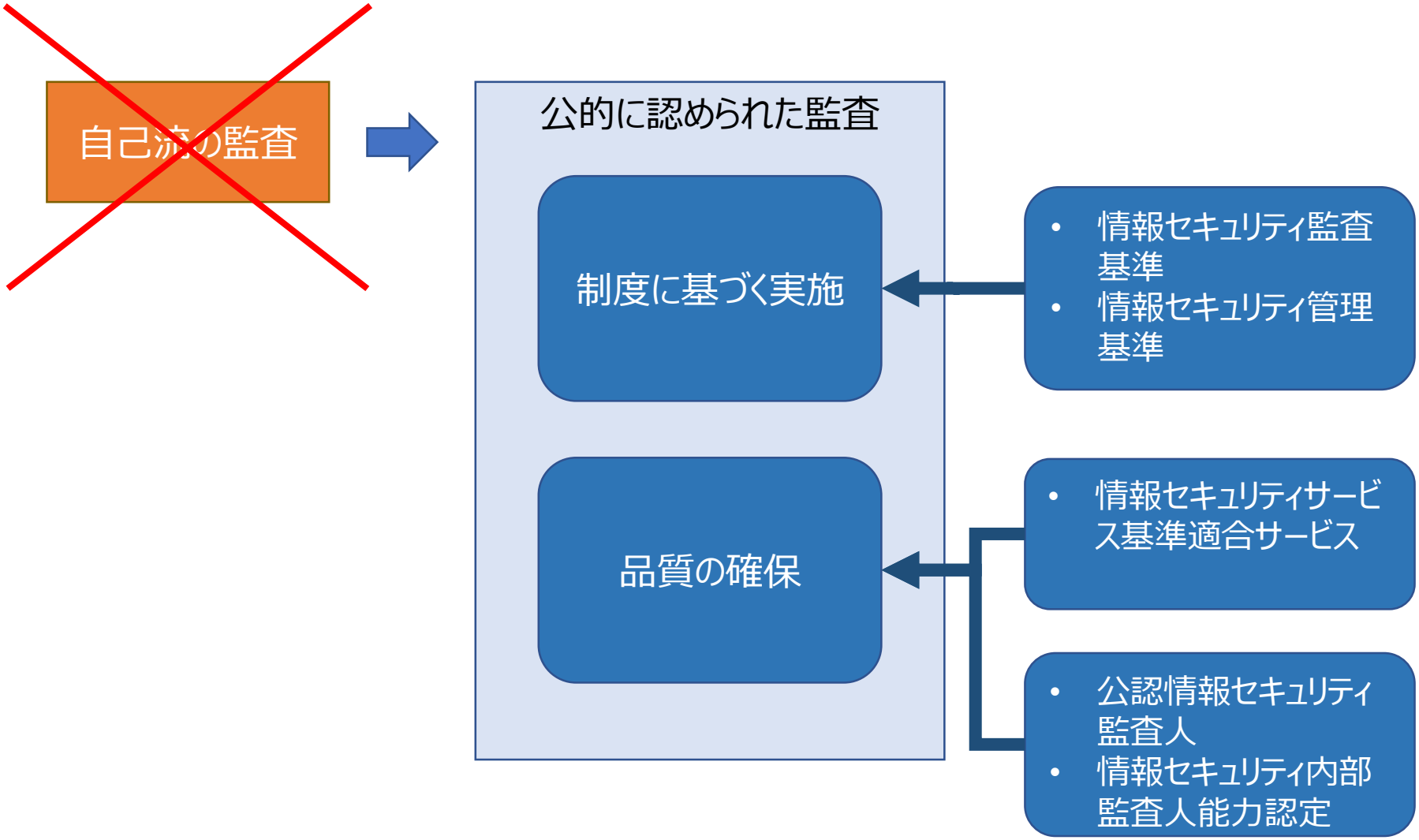
情報セキュリティ監査のしくみ

マネジメントに対する合理的評価のしくみ

要点	解説	具体的内容	必要な人材
基準	基準を満たしているかを判断	情報セキュリティ管理基準※1（個別管理基準）	「情報セキュリティ」と「監査」の知識を共に有する 専門家 （公認情報セキュリティ監査人）
証拠	客観的証拠に基づく事実認識	証拠の評価（証拠能力・証拠力） 証拠に基づくアプローチ	
アプローチ	体系化されたアプローチ	フェーズアプローチ ①方針②計画③実施④意見⑤報告	
評価者	独立した者	行為規範（情報セキュリティ監査基準※2）	
実証	追跡可能なプロセス	文書化：監査報告書、監査調書（情報セキュリティ監査基準※2）	

※１：情報セキュリティ管理基準（平成28年経済産業省告示第37号）
※２：情報セキュリティ監査基準（平成15年経済産業省告示第114号）

活用すべき情報セキュリティ監査



5. サイバーセキュリティの監査

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査

6. 監査役の役割

サイバーセキュリティ監査の確認事項

■企業がサイバーセキュリティに的確に対応できているかの確認
- □リスク認識の共有：組織末端までサイバーリスクの理解が共有できているか？
- □組織態勢の確立：平時も異常時も円滑に全員が動けるか？
- □事　業　継　続　：異常時に事業活動が途切れないか？

■企業態勢がしっかりしているかの確認
- □経営者が役割を果たしているか
  - ◆企業存続に影響するサイバーリスクを常に見直しているか？
  - ◆リスク認識の共有を図っているか？
  - ◆適切なガバナンスを行っているか？
- □管理者が適切に管理しているか
  - ◆PDCAがしっかり回っているか？
- □技術者が適切に対処しているか
  - ◆OODAによりインシデント検知が行われているか？
  - ◆インシデント対応態勢が動くか？

サイバーセキュリティ管理基準

■判断の尺度としての管理基準
- 情報セキュリティ管理基準+サイバーセキュリティ固有の基準

■サイバーセキュリティ対策マネジメントガイドライン
- ISO/IEC27001及び27002とNIST SP800-53の差分を整理
- このガイドラインをベースに個別管理基準を組織に合わせて作成できる
- Ver1.0を公開済み
  （ https://www.jasa.jp/information/public_doc.html ）
- Ver2.0策定中

■ガバナンス基準
- 「情報セキュリティガバナンス導入ガイダンス」（経済産業省平成16年度）に基づき、以下の4つを監査
- 方向づけ（Direct)、モニタリング（Monitor)、評価（Evaluate)、報告（Report)

6. 監査役の役割

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査

監査役の行うべきこと

- 経営者がサイバーセキュリティに適切に対応しているかを利害関係者に説明できるようにすること
  - サイバーリスクが常に見直されているか
  - 組織におけるサイバーセキュリティリスクコミュニケーションができているか
  - サイバーセキュリティのガバナンスが有効か

- 各現場において、サイバーセキュリティのマネジメントが的確に機能しているかを確認すること
  - マネジメント監査が適切に行われているか
  - 監査人の力量（特に技術的な力量）が十分か

参考：情報セキュリティ監査人資格制度
https://www.jasa.jp/qualification/about.html

参考資料

ガバナンスとマネジメント、コントロールの意味

- ガバナンスの語源はラテン語の船を操舵する（gubernare）⇒**方向を示し、導く**
  - 船を操舵するは単に舵をとるという意味ではなく、船に加え、乗組員や船荷に配慮し、暗礁や悪天候の中でも安全に目的地に着くことを意味している。
- マネジメントの由来は「手」を意味するラテン語「manus」⇒**操作して、目的を達成する**
  - もともと何かをモノを扱うという意味である。 その名残として馬を扱う調馬場を指す言葉として「マネージュ」が国際的に使われている。
- コントロールはラテン語の”contrarotulus“に由来する⇒**管理のための目録（具体的な方法のリスト）**
  - "Contra (～に対する)" + "Rotulus (巻物、目録、台帳）"

【独自】行政文書が大量流出　納税記録などのＨＤＤ転売

神奈川ＨＤＤ流出

茂木克信　2019年12月6日05時00分

組織名称	株式会社ブロードリンク
組織部門名称	－
所在地	東京都中央区日本橋室町4丁目3番18号東京建物室町ビル8F
認証基準	JIS Q 27001:2014(ISO/IEC 27001:2013)
認証登録番号	IS 517544
	・中古パソコン・OA機器の買取販売及びデータ消去サービス・オフィス内装工事・情報機器の設定、設置及び修理・産業廃棄物のリサイクル業務（中間処理） 2014年09月01日付適用宣言書 第9版

（出典）ISMSマネジメントシステム認定センター

納税などに関する大量の個人情報や秘密情報を含む神奈川県庁の行政文書が蓄積されたハードディスク（ＨＤＤ）が、ネットオークションを通じて転売され、流出していたことが朝日新聞の取材で分かった。県のサーバーから取り外されたＨＤＤのデータ消去が不十分なまま、中古品として出回っていた。県によると、データの消去から廃棄までを請け負った業者の社員が、転売に関与したことを認めているという。

（出典）https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html