CISO支援WGの これまでと、これから （たぶん）その１

JNSA 社会活動部会 CISO支援ワーキンググループ

JNSA CISO支援ワーキンググループの歩み

- 2015年　現MS河野さんと当時MS高橋で活動を開始
- 2016年　CISO支援ワーキンググループを設立　　“蕎麦屋の出前プロジェクト”と呼ばれる

- 2018年　「CISOハンドブック Ver1.0β」をWebで公表　　https://www.jnsa.org/result/2018/act_ciso/index.html
- 2019年　中小企業向けとして「MY CISOハンドブック」を公表　　https://www.jnsa.org/result/2019/act_ciso/
  JNSA 全国横断サイバーセキュリティセミナー2019向け資料

- 2021年　技術評論社より「CISOハンドブック―業務執行のための情報セキュリティ実践ガイド」を出版
- 2023年　技術評論社より「CISOのための情報セキュリティ戦略」出版
- 机上演習のための「CISO-PRACTSIEワークショップ用マテリアル」を公開
- 2024年　机上演習のための「CISO-PRACTSIEワークショップ用マテリアル Ver2」を公開
  https://www.jnsa.org/result/act_ciso/2024/index.html
- Security Daysでワークショップを開催（３月、１０月）
- 2025年　Security Daysでワークショップを開催（３月）

WGで議論した主要なテーマ

1. 経営とセキュリティへの疑問
   - セキュリティ規範から経営を見るのは正しいのか？
   - 橋渡し人材は経営陣ではない、経営陣としての責務とは?

2. 誰の視点でセキュリティ施策を考えるか
   - ベンダー視点ではなく、監査視点、規範視点ではなく
     事業視点で考えるセキュリティとは?

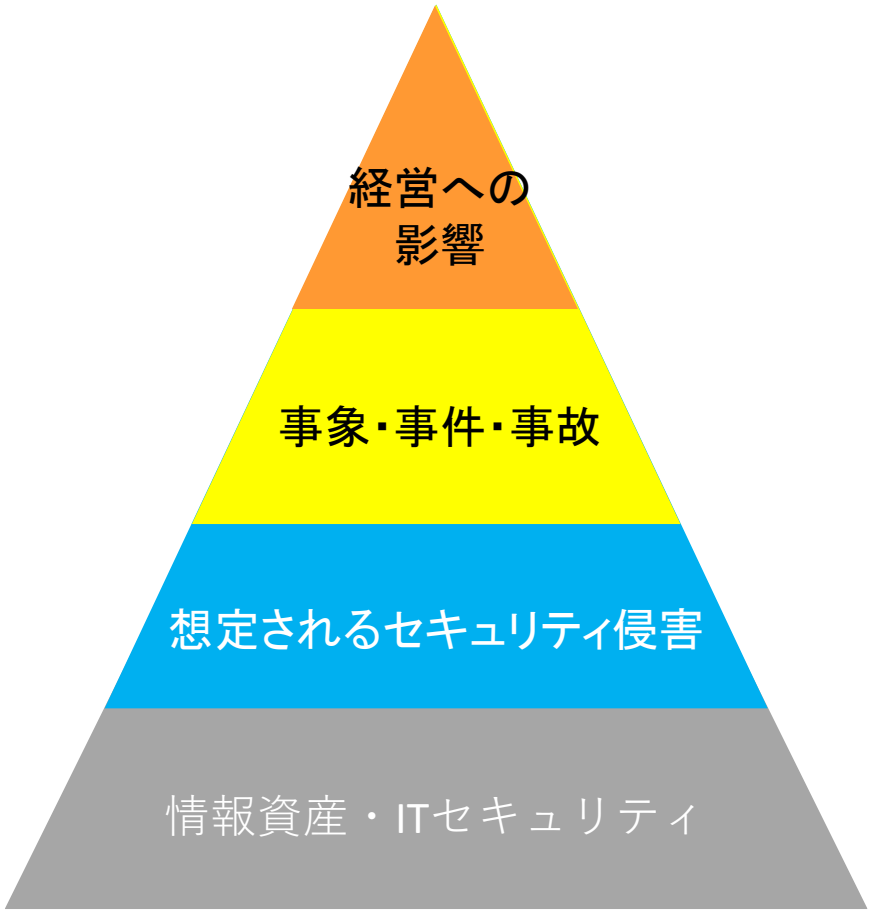
3. 事業計画にセキュリティを組み込むには
   - セキュリティにはインカムがないので原理的にROIは算出できない

4. CISOは育成できるのか
   - CISO-PRACTSIEワークショップの変遷

1. 経営とセキュリティへの疑問

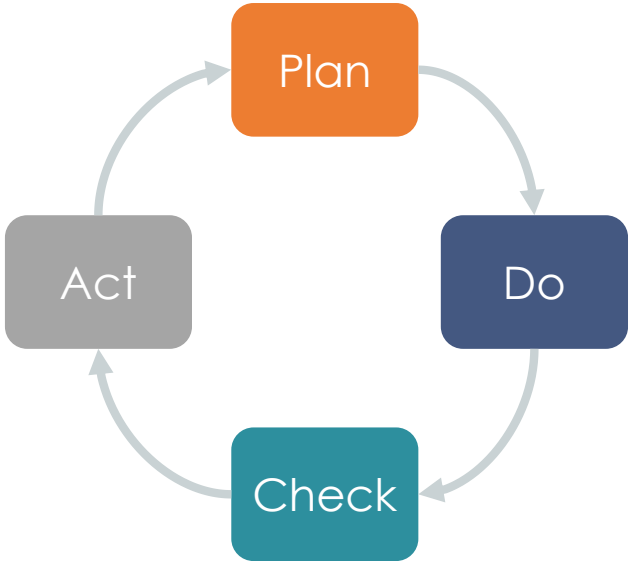
ISMSから経営を語るのは正しいのか？
橋渡し人材は経営陣ではない
経営陣としての責務とは?

ビジネスリスクとセキュリティリスクの関係



Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
競合優位性の低下：競合の躍進、評判の低下 費用的な損失：損害賠償、営業機会損失 事業への影響：営業停止		
ストーキング 秘密の暴露 スパイ行為	システム誤作動 偽の発注・契約 紛争の誘発	システムの停止 社員間の連絡できない 社外との連絡できない 売上が立たない
利用状況の漏洩 画像・音声の漏洩 踏み台による漏洩	プログラム等の改ざん データの改ざん	プログラム等の改ざん 制御データの改ざん 通信経路の遮断
ソフトウェアの脆弱性 設定の不備 プロトコルや暗号の不備 ネットワークや通信の不備	運用上の不備 利用者による改造 認証の不備 ワーム・ウィルス	

プロスポーツで考える事業・経営の構造



計測する対象は、立ち位置によって違ってくる

選手の視点（試合の視点：OODA的）
- 自身の成績、ゲームに勝つ、年棒を上げる
  ポジションや役割によってゴールが違うものになる
- 個人成績（得点・アシスト・打率等）

監督の視点（シーズンの視点：OODA, DevOps的）
- シーズンで成績をあげるためにゲームに取り組む
- 課題は次のゲームまでに改善に努める
- 選手を評価する（個人成績、サイバーメトリックス）
- チームの成績（ 順位、試合数）

オーナーの視点（中長期的な視点：PDCA的）
- チームが存続する価値と収益があること
- コンセプト・経営計画・投資計画・財務状況（経費と収益）

- チームの成績・選手の評価・スタッフの評価
- チームの価値

参考：今こそスポーツチーム経営を考えよう｜橋本 貴智 https://note.com/takatomoh/n/n92441835b7dd

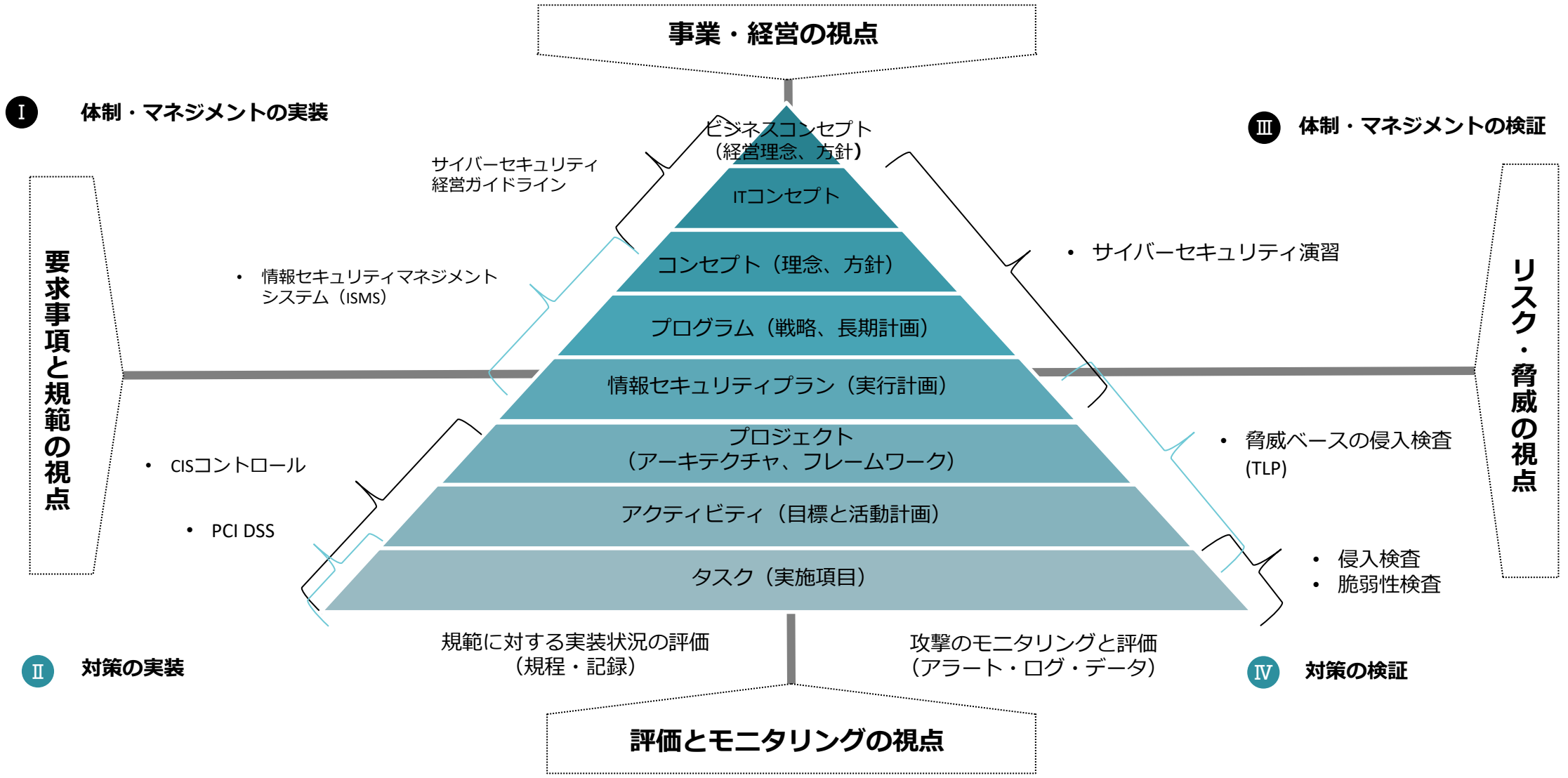
経営とセキュリティへの疑問について

- 経営者がセキュリティを理解すべきか？
- CISOの業務執行とは何か？

2. どこからセキュリティ施策を考えるか

ベンダー視点ではなく、
監査視点、規範視点ではなく
事業視点で考えるセキュリティとは？

チェックリストと構造化アプローチ



料理で考える本講演の論点

料理人としてのシェフ
担当責任者としてのシェフ
経営者としてのシェフ

ソリューションのスキーム

Research
素材と鮮度の探求

Best of breed（最高の材料）
セキュリティ製品・サービス

ここにフォーカスしすぎてないか？

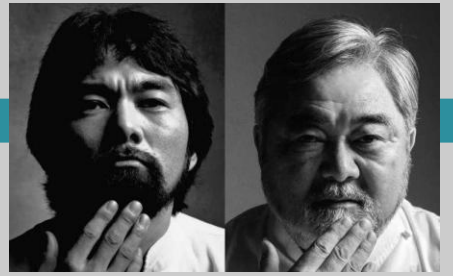
Research
器具と調理法の探求

Best Practice（最高の方法論）
セキュリティ規範・規準

専門家のスキーム

Skilled Operation
熟練の料理人

良い素材x良いレシピ＝良い料理



三流シェフ（幻冬舎） 三國清三

素材とレシピがあれば出来る？

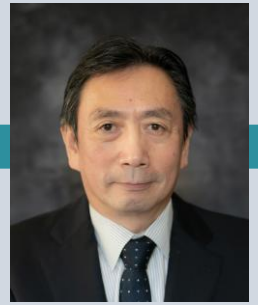
最高！

オーダーは、この料理なのか？

事業（ユーザー企業）のスキーム

Unskilled Operation
非熟練者

良い素材x良いレシピ≠良い料理



CISO

こいつをどうにかしないと
ダメなんじゃないか？

ひどい・・・

結果から考えないとダメ？

どこからセキュリティ施策を考えるかについて

- JNSAの会員企業についても重要な論点ではないか？
  - ソリューションベースの視点は？
  - 監査ベース、規範ベースの視点は？
    - チェックリストをどう思う？
- 業務執行として考えることで整理がつかないか？

3. 事業計画にセキュリティを組み込むには

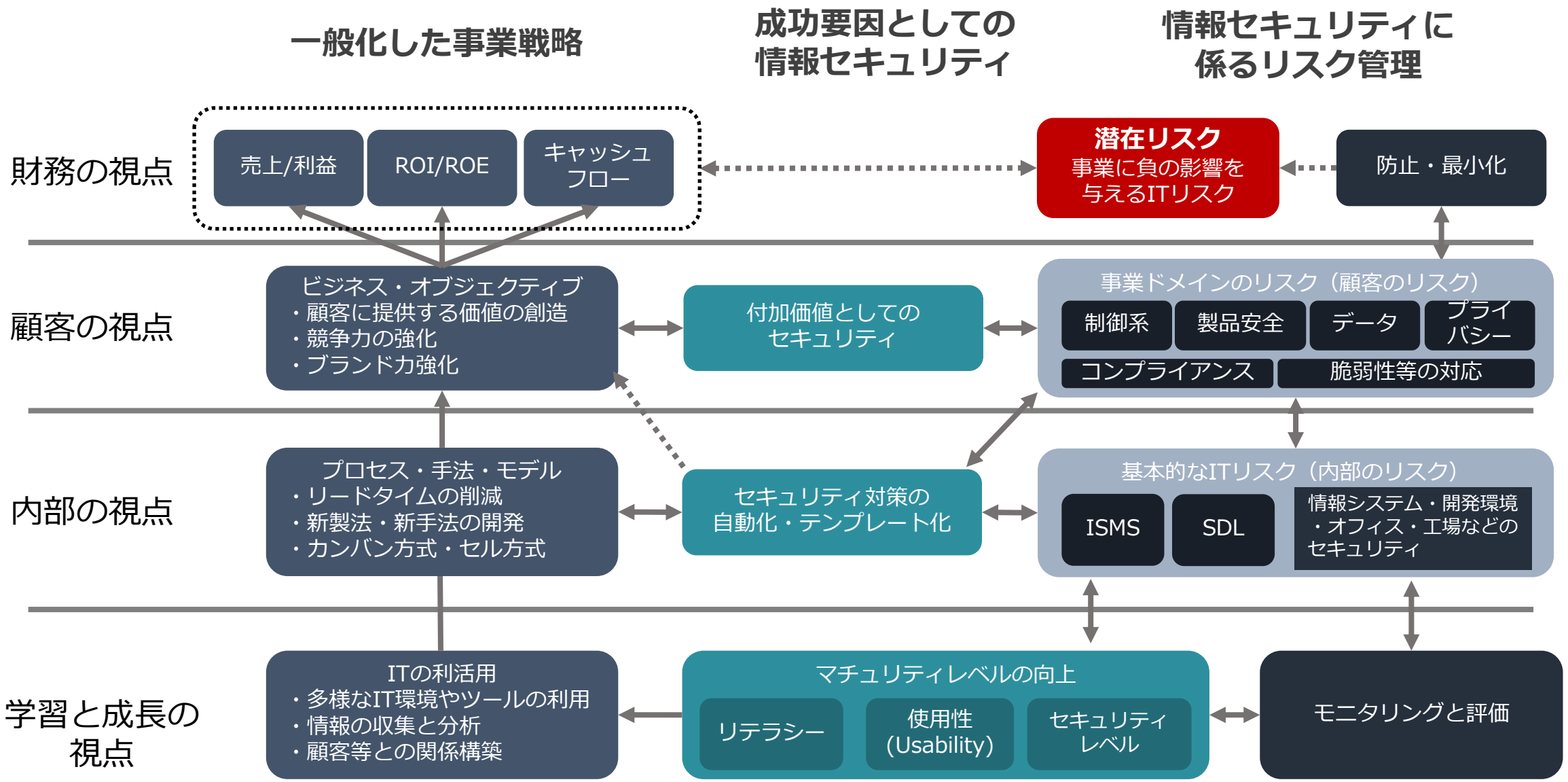
セキュリティにはインカムがないので
原理的にROIは算出できない

CISO支援WG最初の疑問だった

- 組織論ではなく…
- セキュリティ規範の実装ではなく…
- 最新のセキュリティ技術ではなく…

- とりあえず、
  「経営会議で（ちゃんとした）報告が出来ること」とした

成功要因としてのセキュリティ（BSC）



事業計画にセキュリティを組み込むにはについて

- 経営会議で伝えるべき内容と同じ論点か？
- 海外のCISOと日本のCISOで違いはあるか？
- 要するに人と予算が付くということか？
- 成功要因としてのセキュリティはあるのか？
- 事業に関わるリスクをマネージすることか？

4. CISOは育成できるのか

CISO-PRACTSIEワークショップの変遷

CISO-PRACTSIE(ワークショップ)の概要

財務的な目標ではなく、
合理的な公表内容を目標とする

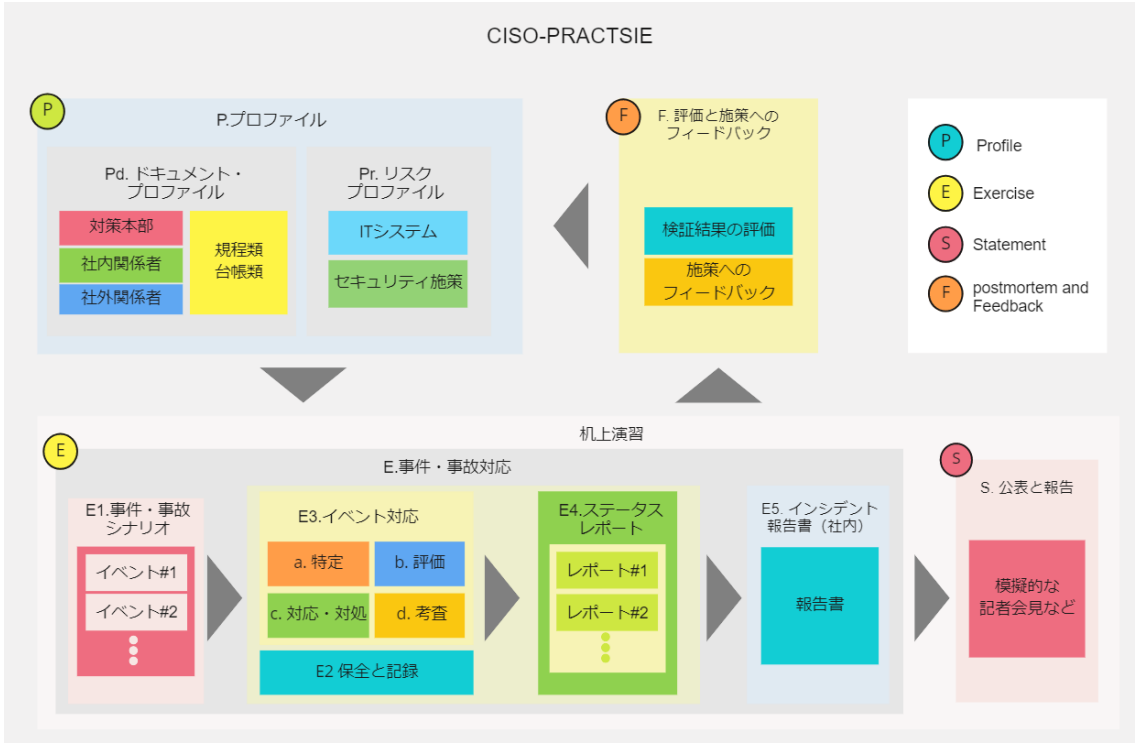
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

INPUT

セキュリティ事件・事故のケース

- 標的型攻撃で**機密情報が漏れた**可能性
- ハッカーの侵入を受けて、**すべてのメールがインターネットに公開**された
- WEBページから**顧客情報が閲覧可能な状態**
- **弊社にしか登録をしていない「メールアドレス**に広告が入った」とのクレーム
- 顧客から、**弊社にしか登録をしていない「クレジットカード**が勝手に使われた」
- インターネット上の**掲示板に弊社の顧客情報**を含むドキュメントが掲載されている
- **弊社**が所有するIPアドレス**から攻撃**を受けているとのクレームが入った
- 弊社のメールアカウントを使った、**標的メールが取引先に送信**された

PROCESS

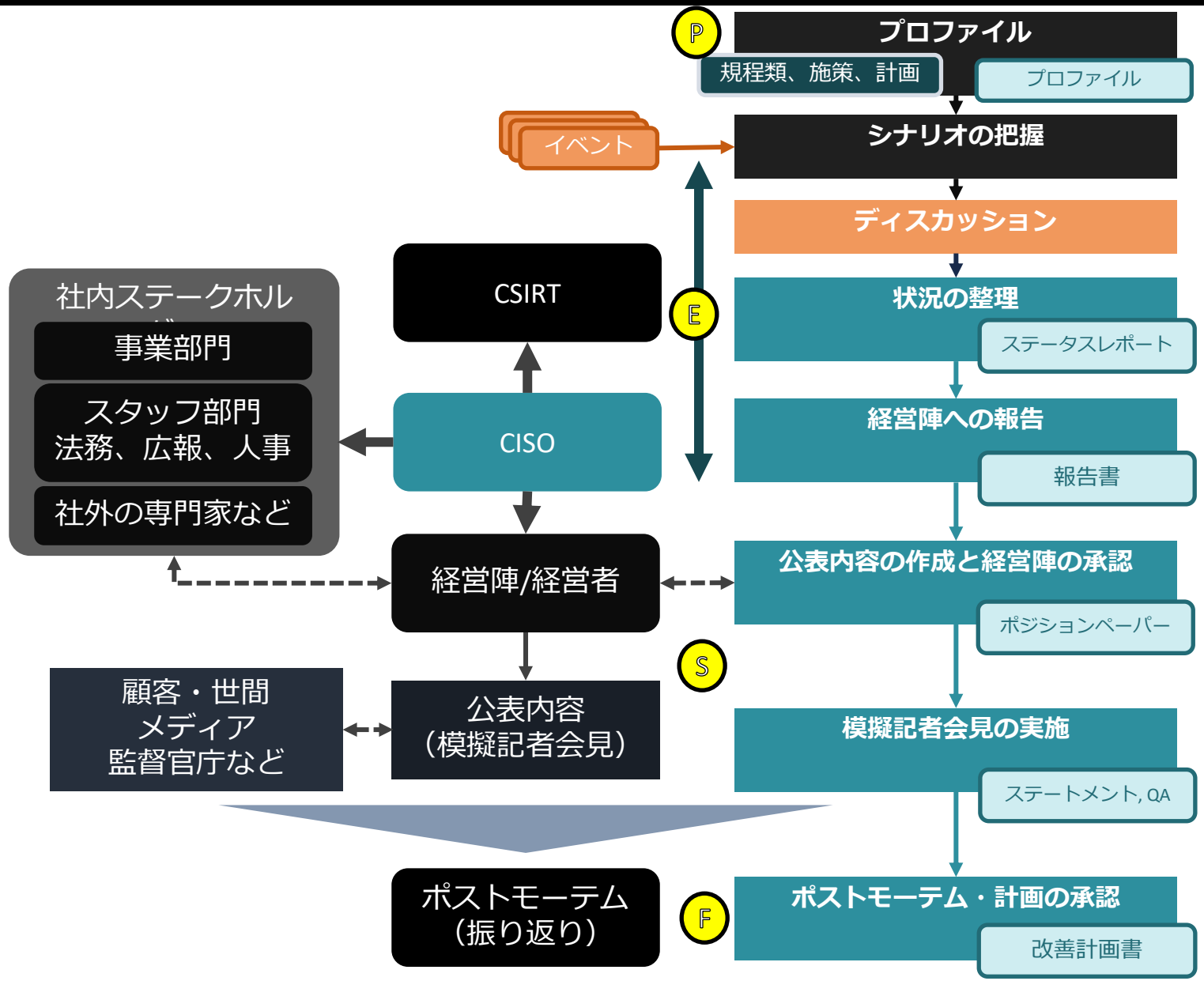


OUTPUT

公表内容：ポジションペーパー	
影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される２次被害
	ワークアラウンド（被害の軽減策）
	被害者への補償
事業への影響	事業の停止・再開の予定と根拠
	事業レベルの対応（営業停止、継続、縮退など）
事件・事故の経緯	事件・事故の原因・要因（なぜ防げなかったのか）
	対応のタイムライン（経営者が認識したタイミング）
再発防止策	再発防止策の内容と実施時期
責任関係	関係者の処分など

CISO-PRACTSIE: PRactical Assessment for Company-wide security measures Through Security Incident Exercise for CISO

CISO-PRACTSIEの流れ



- 会社の状況、セキュリティ施策、経営計画など、対応を行うための基盤となる情報を収集し整理（プロファイル）する

- 提示されたイベント（シナリオ）を理解する

- セッションのウォーミングアップ
- 提示された議題について、意見を交換します

- 関係者に確認する項目を確認し、事業・経営視点で現状況を把握
- この作業を通じて関係者の共通認識を醸成する
- 状況が変化したときは、速やかに内容を更新する

- ステータスレポートに基づいて、経営陣への報告書を作成する
- 単に収集した情報を述べるのではなく、事業や経営への影響を明らかにし、経営陣に求める判断や、依頼事項を明らかにする（費用、リソース、システムの停止など）

- 一般的には広報が作成するが、セキュリティ施策の合理性を検証するためにCISOの立場で作成する
- 防御・対処・検出などの公表内容の証跡について検証する
- ポジションペーパー（≒公表内容）は経営者の承認が必要
- 経営者（役）は会見をする立場から検証し公表内容を仕上げる

- 模擬会見から客観的で合理的な説明が出来ることを検証する。
- 記者役からの質疑応答を通じて、内々の理屈となっていないか、欠けている視点は無いか、などを検証する。

- 対応や改善が必要な項目と対応計画を明らかにする

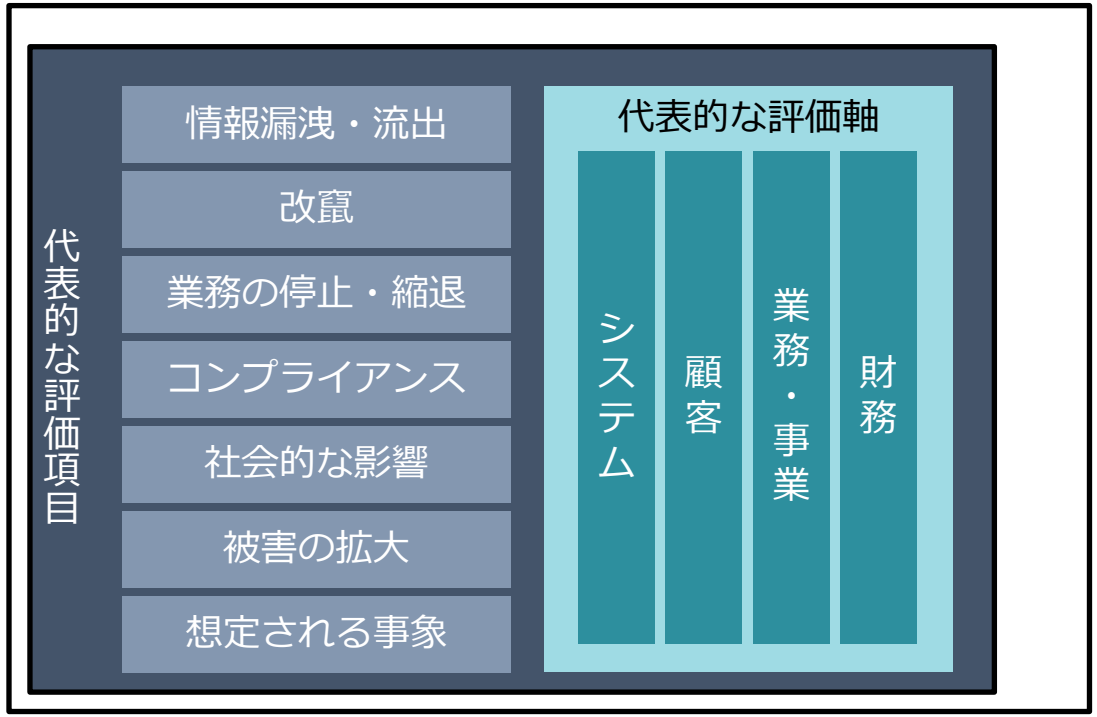
■社内で実施する場合

- 「再発防止策」は「今すぐ実施すべき施策」
- 対応や改善は、「実施計画」に落とし込む

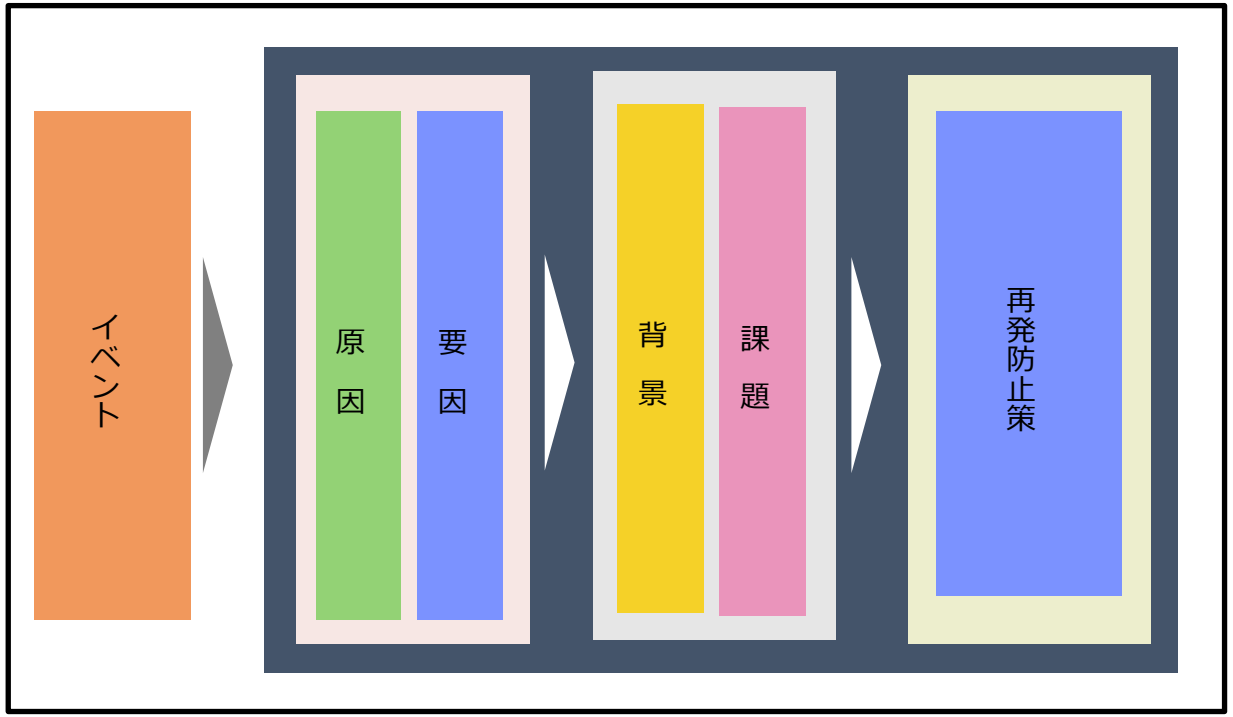
E-b:状況と必要な対応の把握

状況と必要な対応・対処についてディスカッションし、結果を「ステータスレポート」にまとめてください。
影響度、深刻度については、「事業視点でのリスク評価項目」に基づいて、顧客、業務、財務の視点から評価し、「原因・要因・背景・課題」を参考に、技術的な原因だけではなく、組織としての背景や課題についても検討してください。
なお、ステータスレポートに正解はありません。各項目を記載するうえで必要な事柄を考慮して作成してください。

事業視点でのリスク評価項目と評価軸（重要度・深刻度）



原因・要因・背景・課題で分析する



CISOは育成できるのかについて

- ワークショップを通じて、CISOの育成は出来るのか？
- CISO経験者と未経験者の違いはどこにあるのか？
- 修羅場の経験がものを言うのか？
- 会社を代表する（Representative）という概念を身につけるには？

CISO支援WGのこれから


CISO support Working Group
tell me
the Real!
実際問題
どうやってます?
Tell me the Real!
おしえてCISO-WG!


JNSA