第9回 情報セキュリティマネジャー ISACA東京支部 カンファレンス in Tokyo

講演

2021年2月20日
情報セキュリティマネジャーが知っておくべき企業の危機管理

講師：
社会情報大学院大学　教授
ゼウス・コンサルティング（株）代表取締役
白井　邦芳

本日のアジェンダ

- コロナ禍における企業を取り巻く周辺環境
- セキュリティ事故：モデル事例検証
- 情報セキュリティにおける企業の危機管理

コロナ禍における企業を取り巻く周辺環境

コロナ禍での企業人としての行動変容と課題

- フレックスタイム制
- 在宅勤務・テレワーク
- 居住地域を問わない人財採用
- リモートネイティブな業務プロセス体制
- オンライン会議への不慣れさ
- 紙を使用しない文化への移行に身体がなかなか馴染まない
- 参加者と一度も会わないプロジェクトへの違和感
- 顔の見えない人達との絆や信頼性構築の難しさ
- 自身が発した言動が他人に与える評価が確認できないモヤモヤ感
- 発言・討論はあるがコンセンサスや合議が本当にあるのか不明
- メールでの指示が多くなるが、Fire & Forget の失策につながる
- 一日中、外出しない、誰とも会話しない人達が増えつつあり、極度のストレスを抱える

コロナ禍でのコミュニケーションにおけるリスクと周辺環境

- 在宅勤務が増えてソーシャルメディアでの投稿による拡散スピードが極めて高くなっている。
- ストレス下で、投稿内容が偏重的、暴力的なものが増えてきている。
- インフルエンサーによるものでなくても情報は拡散する。
- 風評リスクは不祥事から発生する間接的リスクではなく単体のリスク。
- これまで通用していたソーシャルメディア上での投稿内容に「噂・憶測にはコメントしない」は通用しない。
- 国民目線での懸念はあらゆる業種業態に及び、その専門性を問わない。
- リリースでは論理的回答が求められるが、ソーシャルメディアでの対応は共感的コミュニケーションが重要となる。
- 危機感度が低くなり、「報告・連絡・相談」の遅滞が危機化を招く。
- メディアの情報収集能力も弱体化しており、記事段階で誤認を招くことが多い。事実関係に間違いがあれば速やかに訂正内容を開示する必要あり。
- 対面での情報交換が少なくなり、噂・憶測・伝聞情報・意見・事実などの情報内容の境界線がぼやけてきており、正確な情報収集が難しい。
- 外部からの不正アクセスが多発化しており機密情報等が流出している。
- 標的型メール攻撃等の標的となりやすい。
- ソーシャルエンジニアリングによる情報流出も多発している。

セキュリティ10大脅威2020

出典：独立行政法人 情報処理推進機構セキュリティセンター

「個人」向け脅威	順位	「組織」向け脅威
スマホ決裁の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

セキュリティ関連キーワード

- Cookie
- 脆弱性の悪用
- ドメイン名
- 写真の位置情報
- 二段階認証
- ランサムウェア
- フィッシング詐欺
- キャッシュレス決裁

セキュリティ事故：モデル事例検証

モデル事例：脆弱性の悪用 1-1

アプリケーションフレームワークの脆弱性を悪用

- 企業はアプリケーション製造者・販売者の公表の常態的監視に伴い、IPA（独立行政法人情報処理推進機構）やJPCERTなどの外部セキュリティ会社を通じて情報収集し、速やかに自身のシステムへの影響調査を開始、システムの保全に務める。
- システムの洗い出しを完了し、対策方法の検討を開始、WAF（Web Application Firewall）にて該当する不正パターンによるアクセスの遮断を実施すると同時に不正アクセスの可能性の調査を実施。
- その結果、不正アクセスの痕跡を確認したためアプリケーションフレームワークが稼働しているシステムを全停止、ネットワーク未接続状態にあったバックアップシステムに切り替えを実施。
- その後、脆弱性対策をバックアップシステムに実施し、不正アクセスの事実が判明。
- ここまでにかかった時間は脆弱性が公表されてから数時間、事後の対応としてはこれ以上を期待することは難しいが、標的となった法人の全量の情報が流出するという危機的事態に陥り公表するに至った。

モデル事例：脆弱性の悪用 1-2

アプリケーションフレームワークの脆弱性を悪用

- 本件は、製造者・販売者が公表した原文（英語）をIPA等が日本語に翻訳する際にかかった数時間を狙った「ゼロデイ攻撃」である。
- 翻訳にかかる時間を待っていては当然に防げないし、時差の違いなどで認知が遅れることも許されないのが「ゼロデイ攻撃」の怖さ。
- IDS（不正侵入検知システム）や各種のセキュリティ対策を講じていても、不正アクセスの可能性を認知し、調査を開始したときには情報流出が完了してしまうという課題。
- システム全停止までのスピード感が重要。
- こうした不正アクセスが行なわれた可能性を、それを検知する対策をより完全に実施している企業ほど早く認識し、公表することによる風評等のインパクトは大きいものとなるが、再発防止の観点からは速やかに対処することは最優先事項であるためやむを得ないと言えるだろう。

モデル事例：SNSを利用した機密情報流出 2-1

LinkedInを利用したソーシャルエンジニアリングによる営業秘密情報持ち出し

＜公開情報に基づく＞

- 警察は不正競争防止法違反の容疑で企業の元社員を書類送検。元社員は在職当時、中国企業へ自社の営業秘密に当たる情報を漏えいした疑いがもたれている。
- 犯行は半年前から行なわれ、営業秘密に該当する技術情報を中国企業の社員にメールで送信した疑い。書類送検の容疑は不正競争防止法違反（営業秘密の領得、開示）。
- 元社員は技術開発部門で勤務、営業秘密にアクセスが可能であった。
- 元社員は当時勤務していた社内サーバーから私物のUSBメモリにコピーし営業秘密情報を不正に入手。
- 私用PCとフリーメールを用いて２回にわたり中国企業へ送信。
- 中国企業は元社員に対し、LinkedInを使って接触していた。
- 元社員はLinkedIn上で氏名、社名の他、導電性微粒子の研究に関わっていることを公開していた。
- 中国企業は企業の取引先として元社員に接触。

モデル事例：SNSを利用した機密情報流出 2-2

LinkedInを利用したソーシャルエンジニアリングによる営業秘密情報持ち出し

＜公開情報に基づく＞

- LinkedInを通じて接触後メール等で連絡を交わし、元社員を中国企業の負担で中国へ数回招く。
- 取引先でないことは訪中後判明したが、元社員は在籍したまま中国企業から技術指導として非常勤の技術顧問就任を打診されていた。直接的な金銭授受は確認されていない。
- 元社員は中国企業の社員と技術情報の交換を通じ知識を深め社内評価を高める目的だった。自身の研究の社内評価も不満。
- 中国企業が示した技術は自社にないものだった。
- 技術情報の交換といいながら中国企業から提供された情報は何もなかった。
- 同僚が元社員の不正行為を気づき指摘、その後の社内調査で発覚。
- 企業は元社員を懲戒解雇、警察へ告訴。
- 元社員は容疑を認めており警察は逮捕を見送る。
- 中国企業の関係者が中国本土におり捜査ができず、漏洩情報の使途等は不明。
- 元社員は懲戒解雇後、別の中国企業大手通信機器メーカーの国内事業所に再就職している。

モデル事例：機密情報管理不備 3-1

社長のスケジュール表を窃取、反社会的勢力に転売！

- 元社員が在籍時に社長のスケジュール表（いつ誰とどこで面談する等、居場所等が克明に記載）を窃取し反社会的勢力等に転売。
- 元社員はコンプライアンス担当者で高度なアクセス権を有していた。
- 監査部によるアクセスログ確認で判明。
- 元社員は転職を考え、退職願いを提出していたが、企業は受領を拒否、調査を継続し懲戒解雇。
- 企業は機密情報管理規程はあったが、「最高機密」「重要機密」「社内機密」「グループ機密」等の仕分けが明確ではなく、社長のスケジュール表に対する情報機密性について認識されていなかった。

モデル事例：ランサムウェアで身代金要求 4-1

不正アクセスによる情報漏えい

- 未明より不正アクセスによりシステムに障害。社内のグループシステムの一部においてメールシステムやファイルサーバーなどでアクセスしずらい障害が発生との公表。社内ネットワークを部分的に見合わせる。顧客情報等の漏洩は確認されていない。
- 不正アクセスから14日後、元従業員9名の個人情報と企業情報として販売レポート、財務情報が流出したことを公表。また、漏洩の可能性のあるものとして個人情報（顧客情報・約35万件）、（従業員、関係者・約1万4千人）、企業情報（売上情報、取引先情報、営業資料、開発資料等）を公表。クレジットカード情報を保有しておらず漏洩していない。
- 71日後、新たに個人情報16,406人の漏洩を確認、また、漏洩可能性のある採用応募者情報 約5万8千人を公表。
- サイバー犯罪集団が自らのウェブサイトで企業から盗んだデータだと主張するファイルを公開し、身代金としてビットコイン1,100万ドル：約11億5千万円を要求。企業側は現時点で支払を拒否。

モデル事例：Ragnar Locker 5-1

サイバー犯罪集団の手口：データの盗取と暗号化解除で身代金要求

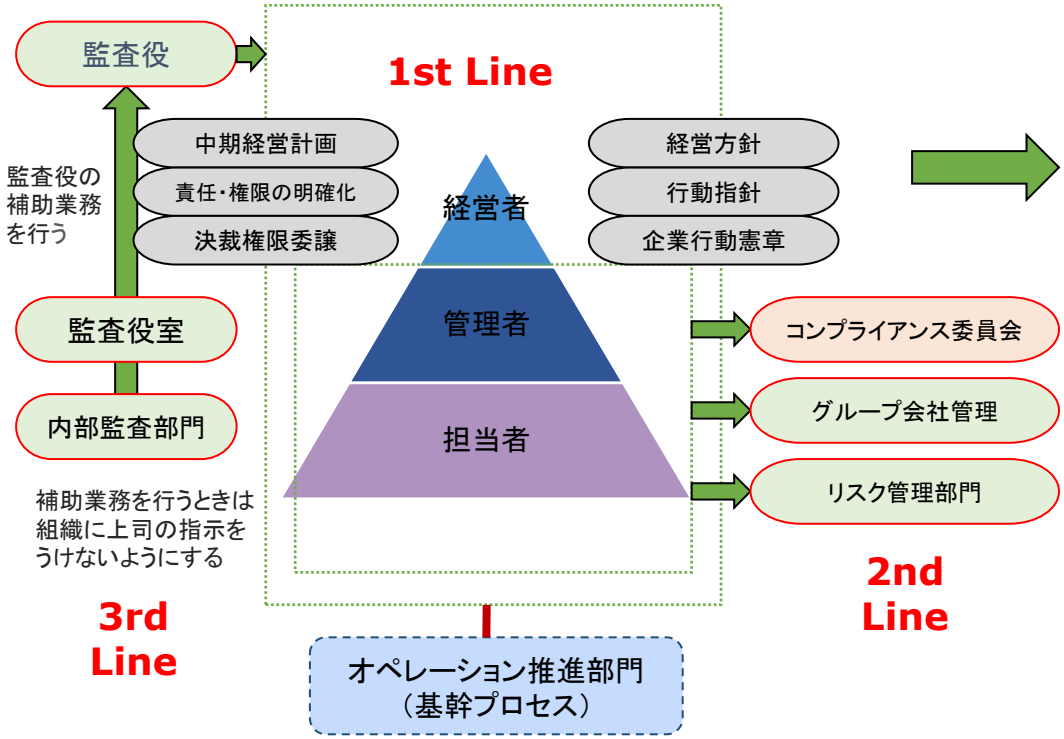
- サイバー犯罪集団はロシア拠点の「Ragnar Locker」と想定。
- 被害企業は各国の法令に従う。
- 不正アクセスは、システムネットワークの操作や機能に影響を与える。
- サイバー犯罪集団の目的は、データの盗取と暗号化解除の対価（身代金）。
- 多くの攻撃対象が米国国内であったため、基本は米国のFBIとの捜査協力となっている。FBIの基本方針は「支払拒否」だが100%支払拒否（違法対処）ではない。
- 攻撃を受けた企業のうち、多くは現地オペレーションに大きな問題がなければ支払を拒否している一方で、一部は身代金を払ったとの情報がある。
- 企業情報のみが盗まれた企業は捜査上の理由で公表を控えている。
- 身代金は日本円にして数億円から数十億円に上るものがある。
- サイバー犯罪集団は身代金の交渉を一定期間継続してくる。弁護士を通じて交渉可能。

情報セキュリティにおける企業の危機管理

会社法に基づく内部統制下の役割と責任
3 Lines of Defense（相互監視）

会社法施行規則100条では9つの統制要件の体制構築が義務付けられました。しかし、この体制作りを行うことが目的ではありません。実効の上がる体制とするためには、各組織の役割と機能分担を整理し、各組織で実行レベルに落とし込む取組みが不可欠です。

内部統制の体制イメージ



内部統制構築に向けた「リスク管理」をめぐる責任と役割の考え方（例）

主体	役割（目的）
取締役会	✓経営者が有効な事業リスク管理を確立したかどうかを管理する。 ✓経営者と事業リスクの現状を認識する。
経営者	✓事業リスク管理についての直接の責任者。 ✓自社のリスク管理能力を把握し、更なる評価が必 要かどうかを判断する。
リスク管理部門	✓複数の子会社や部門をまたぐ形で、事業 リスク 管理全般の実効を支援する。 ✓事業リスク管理が有効に機能するために は、現場の責任者が事業リスク管理の第 一人者となる 必要がある。
財務オフィサー	✓財務経理関連のオフィサーとスタッフは、企業全体の予算策定に携わり、業務・法 令遵守・財務報告の観点から業績を見る役割を持つ。 ✓最高財務責任者（CFO）・最高会計責任者（CAO）は、不正な財務報告を防止し察知する際に重要な役割を果たす。
内部監査人	✓事業リスク管理に有効性を評価し、必要な改善点 を指摘する任務を負い、それにより経営者・取締役会を支援する。 ✓監査対象となる業務から独立し、自らが対象としている事業リスク管理の範囲が適切か考察すべきである。

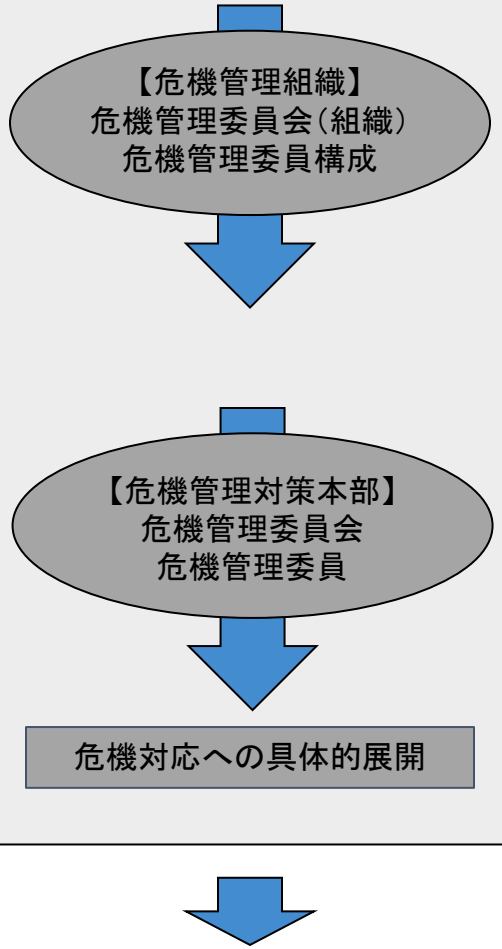
危機管理を取り巻く組織と規程 1

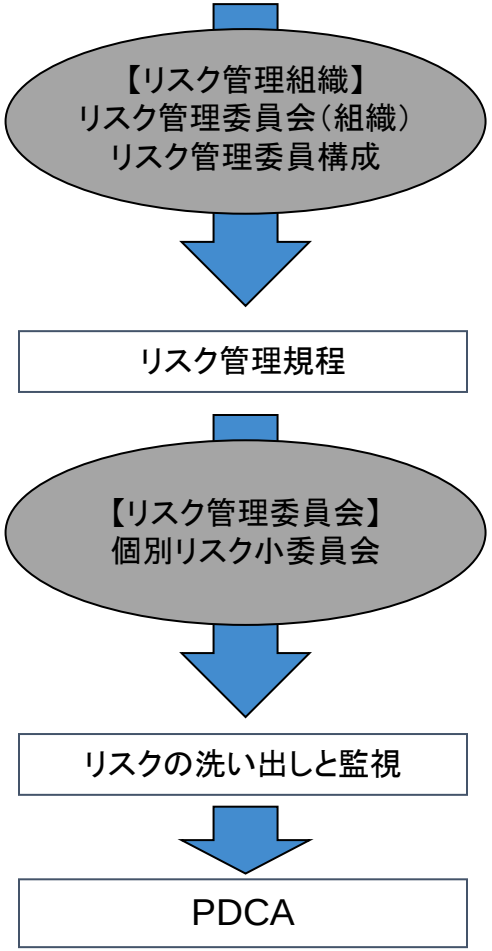
統合リスク管理基本方針（リスク管理基本方針＋危機管理活動方針）

【定義付け】
危機管理の活動趣旨・理念・体制・組織の在り方を規定し、対応事案ごとにおける個別危機管理委員の構成を定める。

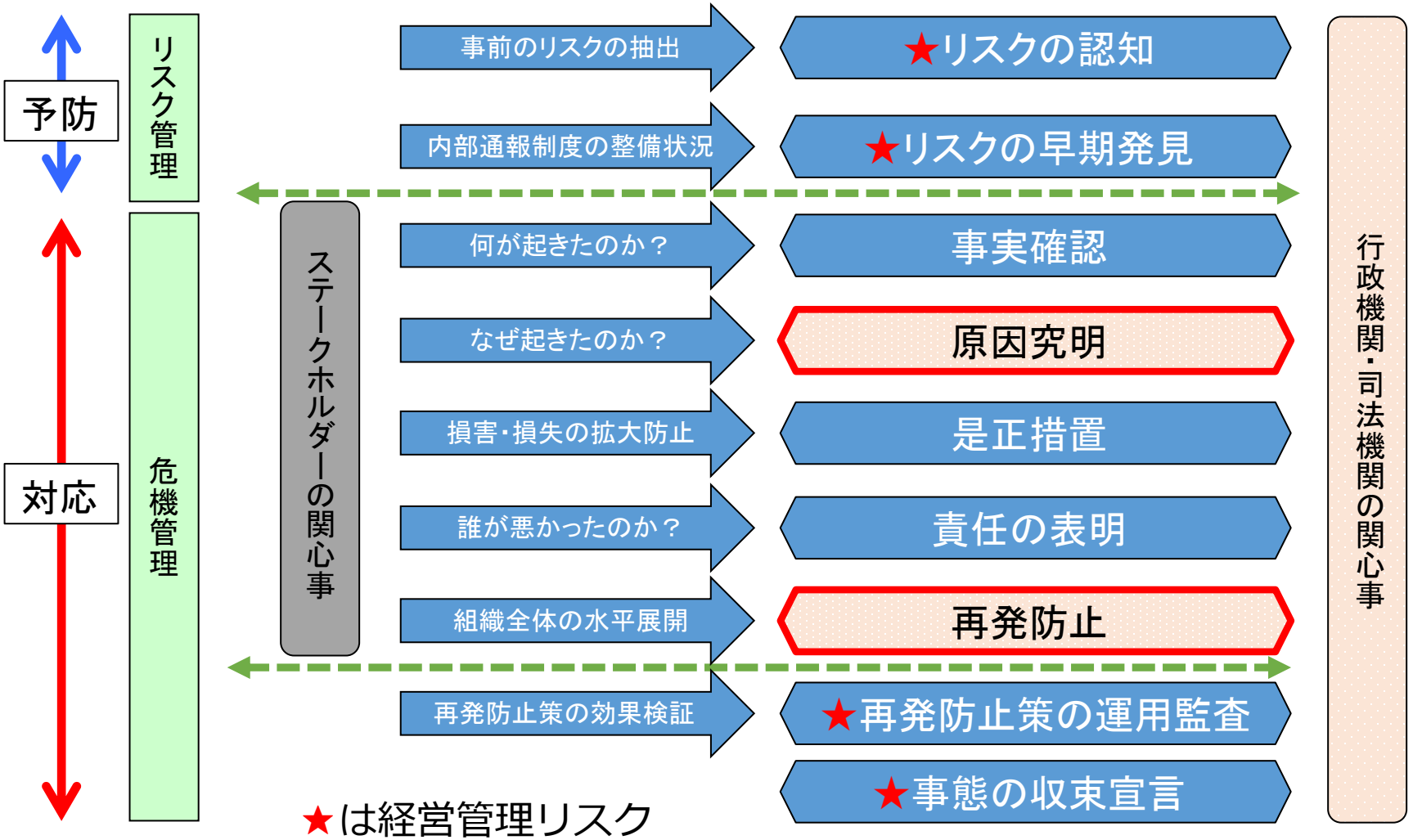
【対策本部設置・招集】
「経営危機の範囲」を定め、危機時の行動の基準、報告、対応の原則、行政への届出、危機管理対策本部の設置と取締役会の招集、危機管理委員会の人事及び責務等について定める。

【外部専門家の登用、第三者委員会】
必要に応じて外部専門家の登用、第三者委員会の設置の検討。





危機管理広報の重要管理視点



行政・司法リスクの危機管理の重要性

【企業が求められている前提事項】
法令遵守のための体制整備

①経営管理等に関する事項

②業務の遂行にあたっての事項

社内体制不備

個別事項違反

遵守体制の重大な欠陥

①行政処分、社名公表、罰則等

②業務停止、継続的業務改善対応

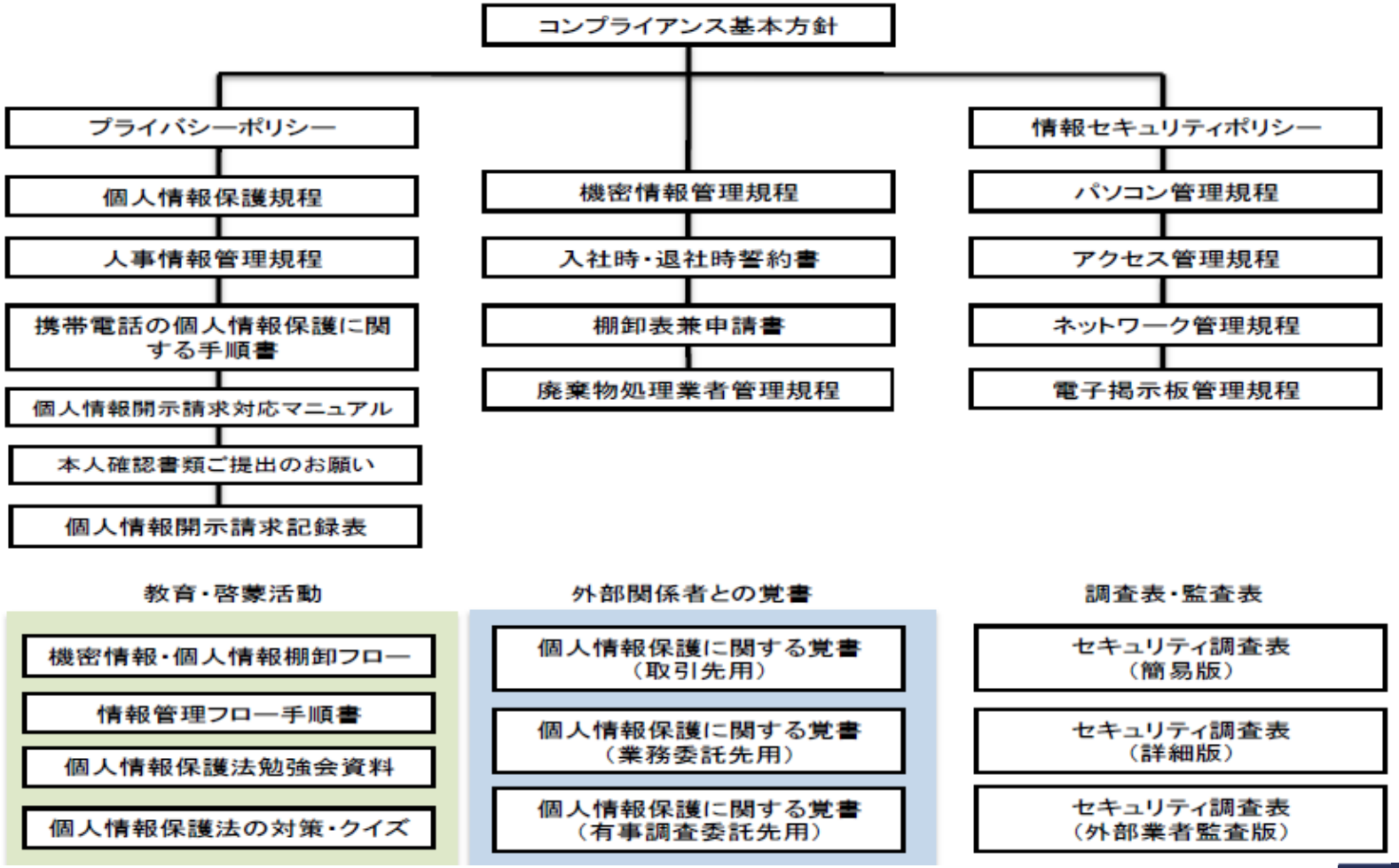
風評・信用毀損

これらの危機的事態を回避するための施策（内部統制システムの整備強化）

①事前予防としてのリスクマネジメント　②事後措置としての危機管理　③適切な公表

規程群の整備（リスク管理用）

個人情報保護の対応規定・手続き



規程群の整備（危機管理用）

個人情報漏洩時の対応規定・手続き

個人情報流出後の行政への届出項目

- ❖報告者
- ❖報告日
- ❖連絡先
- ❖事業者名
- ❖発覚日
- ❖事案の類型と概要
  - a. 不適切な運用（16条、23条）　b. 安全管理措置（20条）　c. 従業員の監督（21条）、
  - d. 委託先の監督（22条）　e. 内部犯行　f. 盗難　g. その他
- ❖流出データの媒体、項目及び件数
- ❖警察届出の有無
- ❖経緯
- ❖2次被害の有無、有の場合の被害拡大の可能性
- ❖本人（情報主体）への対応
- ❖事案の公表の有無、有の場合の内容、スケジュール
- ❖事案の原因究明と是正策、再発防止策（社内外対応）の整備状況
- ❖再発防止策の水平展開の進捗状況

行政への届出後の要請補完資料

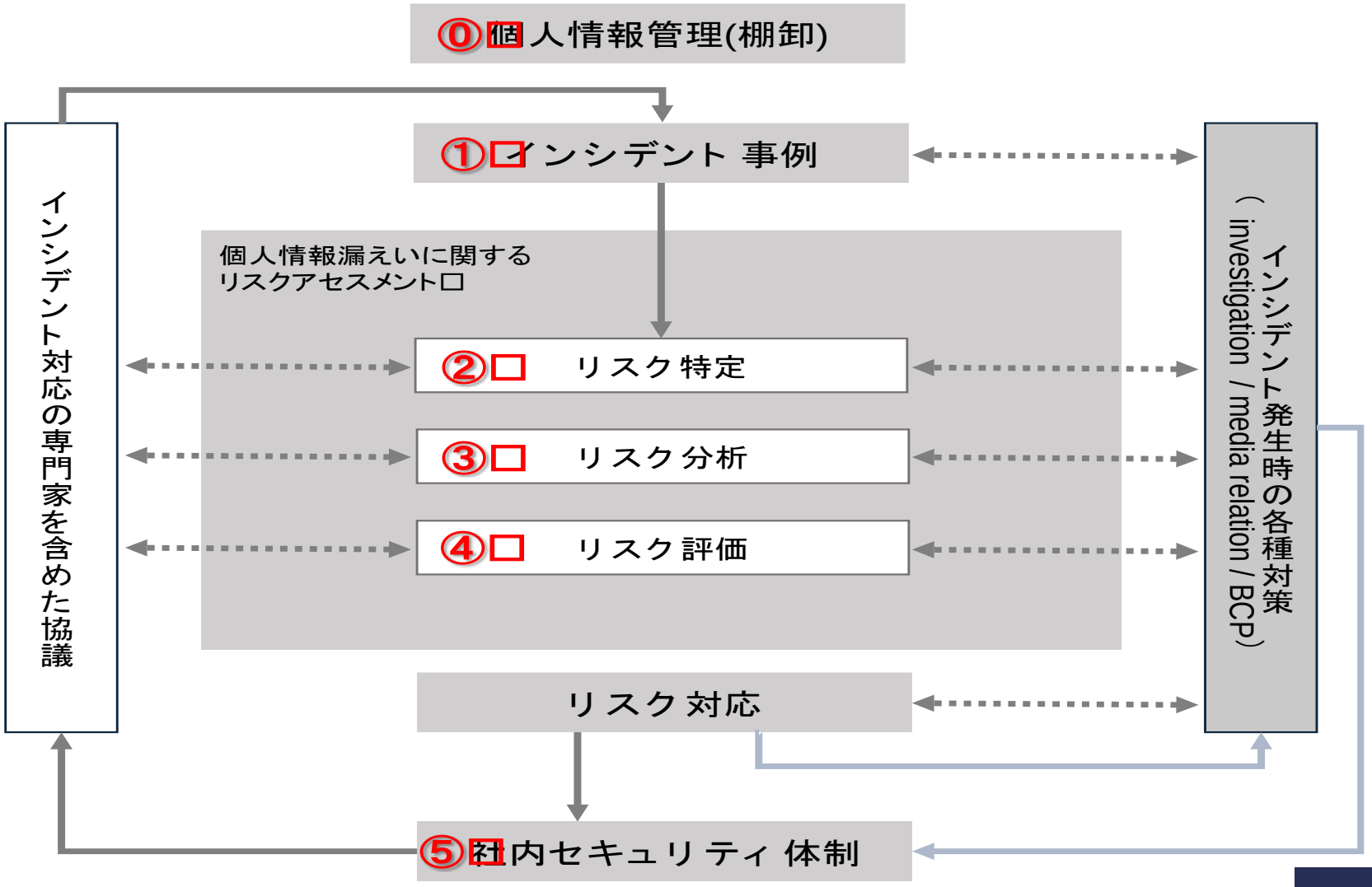
- ❖個人情報保護組織
- ❖有事後の危機管理組織（対策本部）図
- ❖個人情報保護管理規程
- ❖外部業者管理規程
- ❖監査方法に関するルール、過去の実施資料
- ❖個人情報漏洩対応マニュアル
- ❖公表基準
- ❖対策本部設置基準
- ❖教育システムについての実施状況
- ❖各安全管理措置への対応状況
- ❖個人情報保護に関する経営の関与状況

行政からの要請資料の提出懈怠や虚偽報告は、個人情報保護管理者に対しても大きなリスクになるばかりか、会社そのものの大きなリスクとなることも想定される。一例としては所管省庁や金融庁からの改善命令、金融商品取引所からのヒアリング、外部監査法人の財務報告内部統制報告書に対する不適正意見や不表明などのリスクに及ぶことがある。

機密情報の管理

分　類	情報種別	保存期間（年）	文書の名称例	情報区分
内部管理	①取引先調査に関する情報	10	取引先調査依頼書、結果報告書	重要機密
	②個人情報管理に関する情報	10	個人情報管理台帳	重要機密
	③文書保存管理に関する情報	3	文書件名簿	重要機密
子会社管理	①事業計画等に関する情報	10	事業計画、総合予算	重要機密
		15	中期経営計画	重要機密
	②決算に関する情報	15	年次決算、月次決算	重要機密
	③その他管理に関する情報	10	管理資料	重要機密
訴訟・法務	①訴訟・訴願に関する情報	15	訴状　答弁書　判決文　和解調書	重要機密
登記		5	仮差押決定書（第三債務者）	重要機密
関　係			上申書	重要機密
	②係争に因する情報	10	事件簿　個別事件ファイリング	
			協議依頼書	
		5	企業調査書	
	③その他法務一般に関する情報	10	契約書式	
	④不動産登記に関する情報	15	登記済証（権利証・登記識別情報）	
会　議	①取締役会に関する情報	15	取締役会議事録	最高機密
			取締役会議案	最高機密
	②監査役会に関する情報	15	監査役会議事録	最高機密
			監査役会議案	最高機密
	③経営会議に関する情報	15	議事録　議案	最高機密

情報セキュリティ体制整備の全体像（イメージ）



インシデント事例の列挙

想定される個人情報漏えいの一例

リスク	事故例	現状の対策	課題
メール管理	電子メールの誤送信によるアドレス・添付資料・本文に記載の個人情報流出	上司の承認後送信するルールあり	上司の承認手続きの形骸化
物品管理	個人情報の入ったPC端末の紛失	BIOS・Windowsの二重パスワード	パスワード変更が不定期
	個人情報の入ったスマートフォン端末の紛失	パスワード設定、遠隔消去の対応可能	紛失届のタイミングが未周知
	個人情報の入った廃棄PCからの情報漏えい	一般的なデータ消去ソフトの使用	過去の調査不可 復元の可能性も残る
	個人情報の入ったUSBや記憶媒体の紛失	未対策	基本的な使用ルール、セキュリティ対応急務
不正アクセス	アクセス権を有する同僚からパスワードを聞き出して個人情報DBへ不正アクセス	未対策	パスワード変更が急務 社内ルールと処分規定も設置急務

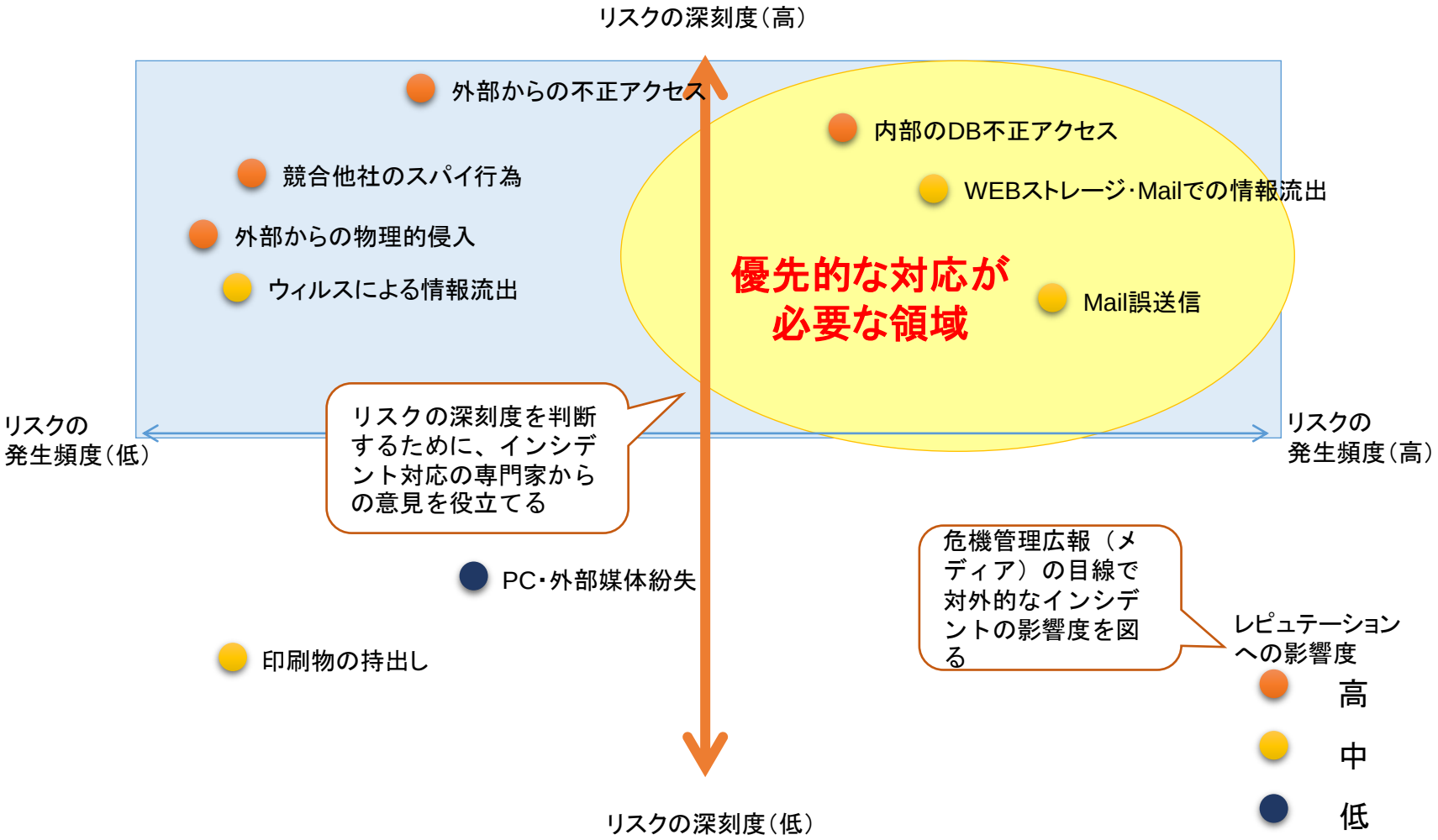
この枠は、ヒアリングやディスカッションで把握

リスク評価の手法とアウトプットイメージ①

業種・業態に即した “個人情報漏えい事例”を作成し、以下の内容を診断結果の基本アウトプットイメージとする。

リスク	リスク値	説明	課題	対応策・発見
洗い出したリスク	リスクの評価の結果を数値（ランク分け）化	リスクの内容について説明	現状の課題	具体的な対応策 (ITセキュリティ対策は別途専門家を要する)

リスク評価の手法とアウトプットイメージ②



ご清聴ありがとうございました。

ご質問等ございましたら、直接以下にご連絡ください。

k-shirai@zeus-c.com