Japan Information Security
Management Systems User Group

脱・形骸化！ISMSを動かすための「実効的マネジメントレビュー」実践論

JNSA 標準化部会
日本ISMSユーザグループ　リーダー
インプリメンテーション研究会　主査

2025年 12月5日

魚脇　雅晴

自己紹介

魚脇　雅晴

NTTドコモビジネス株式会社　情報セキュリティ部サイバーセキュリティ部門
CISSP

JNSA 標準化部会 日本ISMSユーザグループリーダー
インプリメンテーション研究会　主査

現在、JNSA（日本ネットワークセキュリティ協会）の標準化部会の日本 ISMS ユーザグループのWG リーダー及びインプリメンテーション研究会主査としてISMS の規格要求事項の実装方法（サイバー攻撃やクラウド利用などの最新のリスク対応）をテーマとして活動し、毎年、情報セキュリティマネジメントセミナーとして標準化動向や研究会の成果を情報発することでISMS の健全な普及、促進活動を継続中。また、これまでにJASA（日本セキュリティ監査協会）でキュリティ評価基準の検討やクラウドセキュリティ監査制度の検討 WGに参画

本日の説明の概観

具体的なインプット事例として

事例1：AI利用の急速な拡大
事例2：無差別なランサムウェア攻撃の増大

マネジメントレビューとは？

全体像と規格要求事項

インプット情報

内容＆関連条項
具体的な事例紹介

アウトプット情報

アウトプット情報とその影響

有効なマネジメントレビューを目指して

課題と考慮事項
ベストプラクティス

まとめ

マネジメントレビューの全体像と規格要求事項

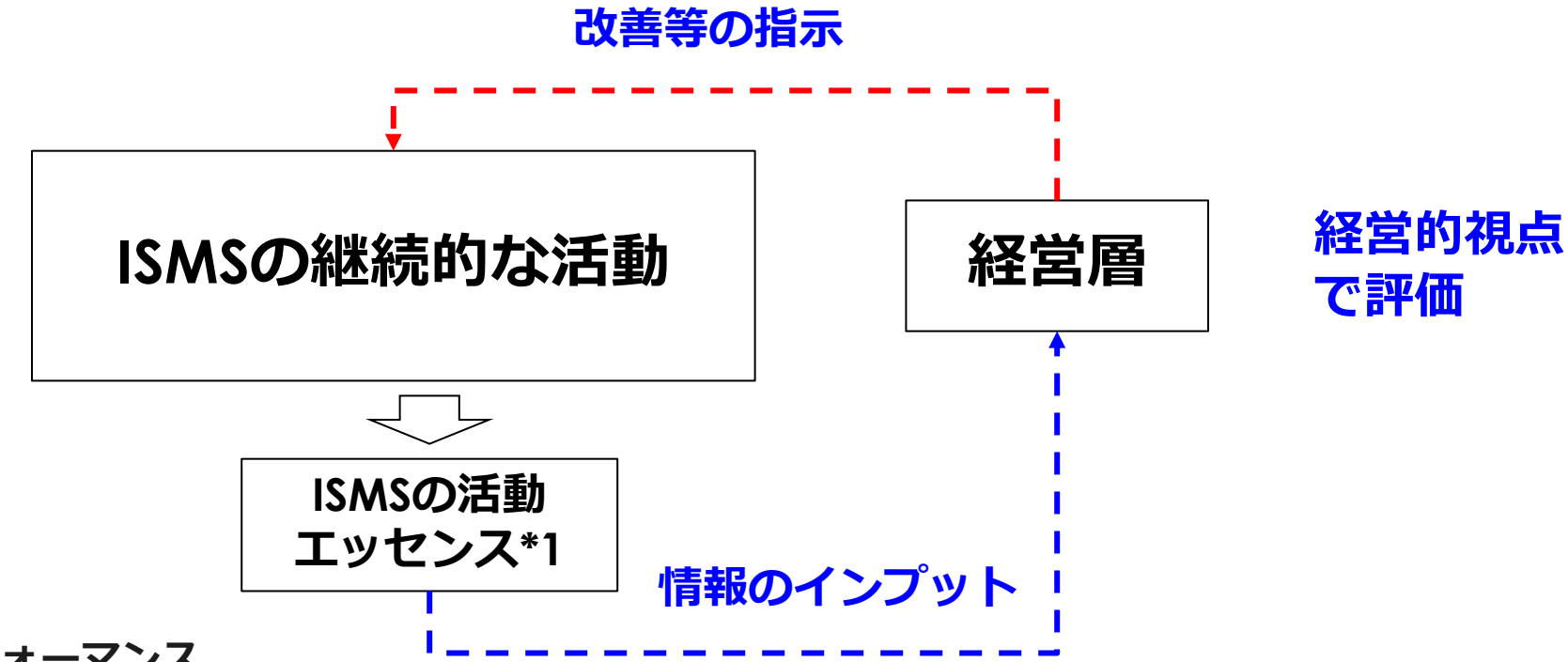
マネジメントレビューは、

ISMSが組織の戦略的方向性や変化するセキュリティ上の要求事項に沿っているかを確認する上で極めて重要な営みとなっています

皆さんの組織では
どのように実施されていますか？

マネジメントレビューについて
（経営層との連携による組織的な取り組み）

・経営層とのコミュニケーションが重要
・経営戦略的な観点での示唆
・良質なインプットと判断、アウトプットの予実管理



*1：ISMSのパフォーマンス
に関する様々なデータ

マネジメントレビューの全体構成

下記のようにトップマネジメントがISMSの有効性を評価し、必要な意思決定を行う場としてマネジメントレビューが実施されている

インプット情報に基づき**経営的視点で判断＆指示**

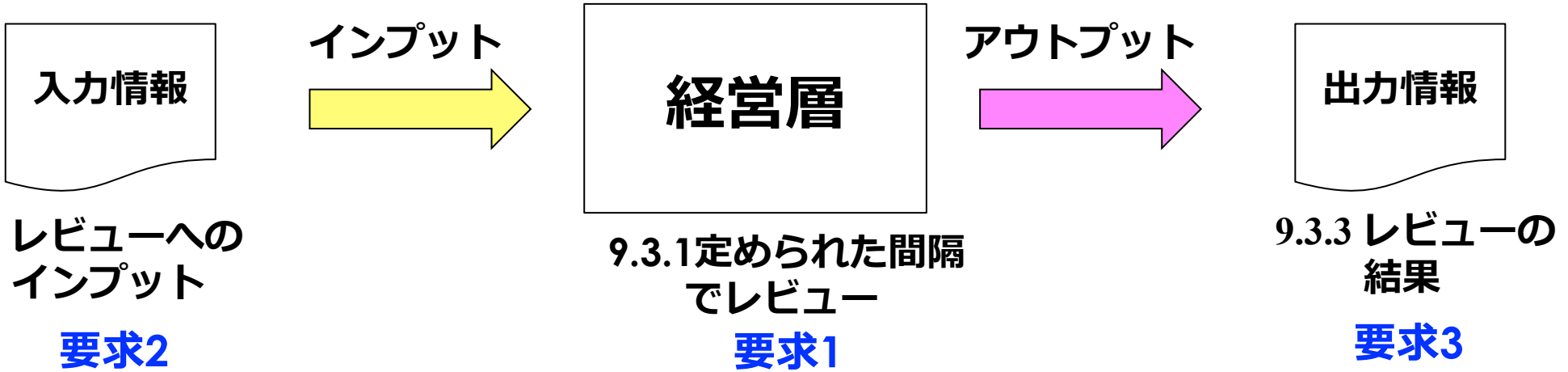
- 情報共有（インシデント、脅威情報）
- 活動計画策定＆変更の承認（予算＆人員の確保）
- リスクの共有（認識＆是正判断）
- 前回の指示事項の予実管理　など

- 改善指示
- 方針、計画見直し

⇩

文書化

規格要求事項から見たマネジメントレビューの全体像



a) 前回までのレビューの結果講じた処置の状況
b) 外部及び内部の課題の変化
c) 利害関係者のニーズ及び期待の変化
d) 情報セキュリティパフォーマンスに関するフィードバック
   1) 不適合及び是正処置
   2) 監視及び測定の結果
   3) 監査結果
   4) 情報セキュリティ目的の達成
e) 利害関係者からのフィードバック
f) リスクアセスメントの結果＆リスク対応状況
g) 継続的改善の機会

・継続的改善の機会，及び ISMS のあらゆる変更の必要性に関する決定
・証拠として文書化した情報

9.3.1定められた間隔でISMSをレビュー

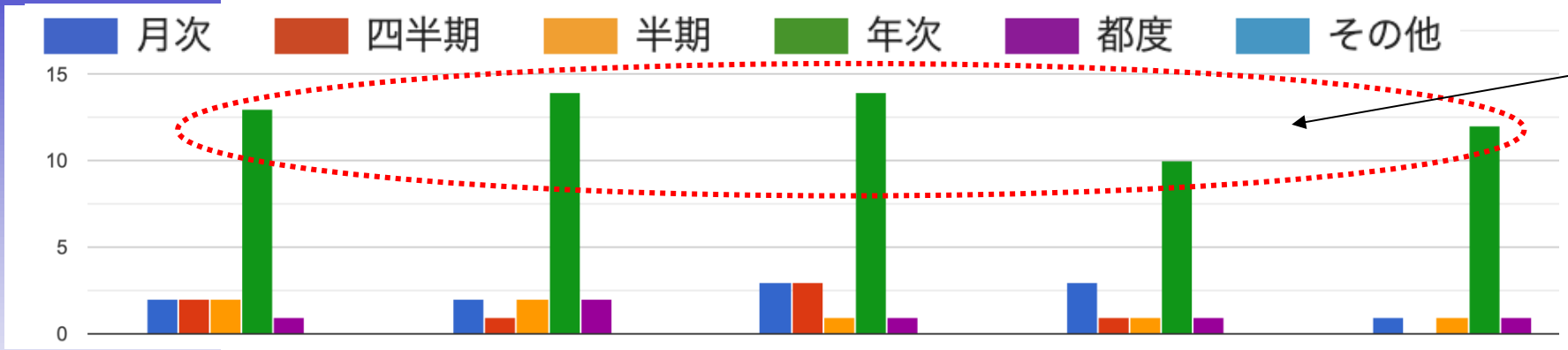
9.3.1定められた間隔とは？

具体的な運用実態についてアンケートで
確認してみました

アンケート結果
（次ページ）

参考資料

マネジメントレビューの議題（トピック）と付議のタイミングの実態



a)前回までのレビュー結果

b)外部、内部の課題の変化

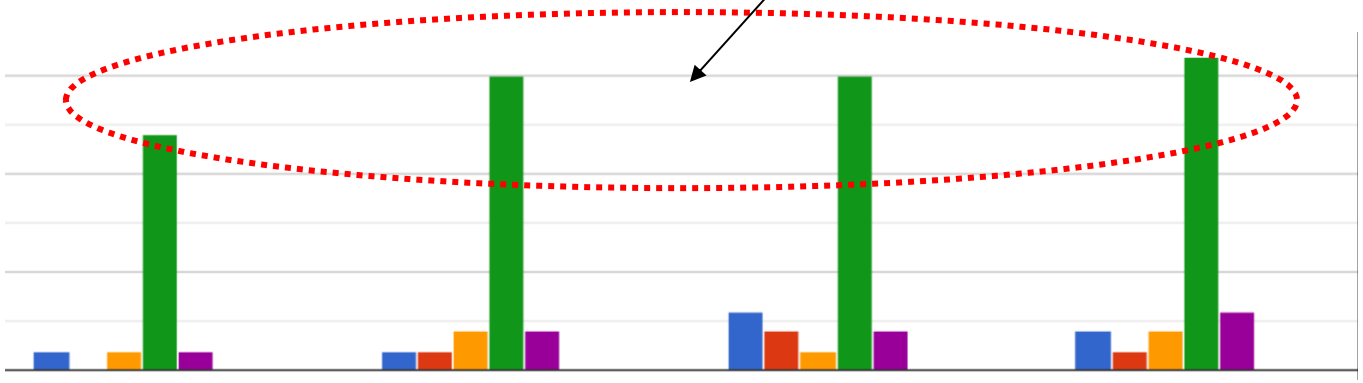
d)情報セキュリティパフォーマンス
1)不適合、是正

d)情報セキュリティパフォーマンス
2)監視、測定結果

3）監査結果

付議のタイミングは年次が主流

経営層は忙しいため、まとまった時間は取りにくい
年1回のイベント的なマネジメントレビューとなっている



d)情報セキュリティパフォーマンス
4)目的の達成

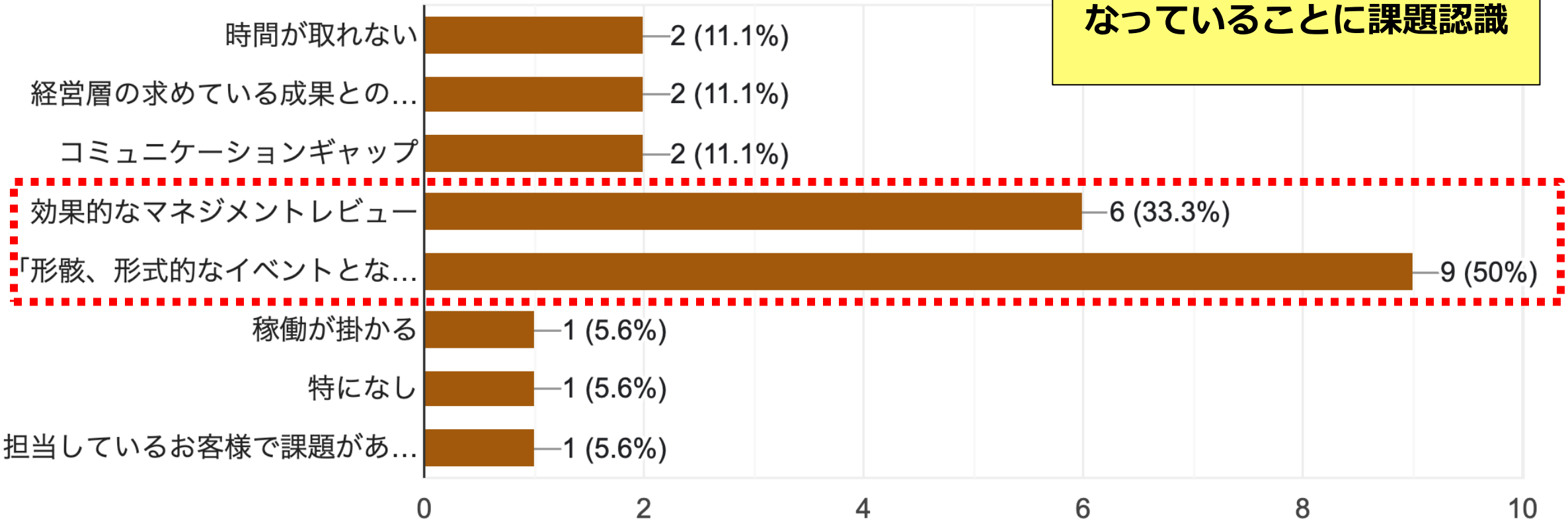
e)利害関係者のフィードバック

f)リスクアセスメントの結果、対応状況

g)継続的改善の機会

マネジメントレビューの課題について

形骸化、形式的なイベントとなっていることに課題認識



事例紹介：マネジメントレビューが年1回の謎について

事実　マネジメントレビューはほとんどの組織で年1回の開催（アンケート結果）

背景　必ず経営層のトップを交えた打ち合わせの場をセットしなければならない、
経営層は忙しいため、まとまった時間は取りにくい

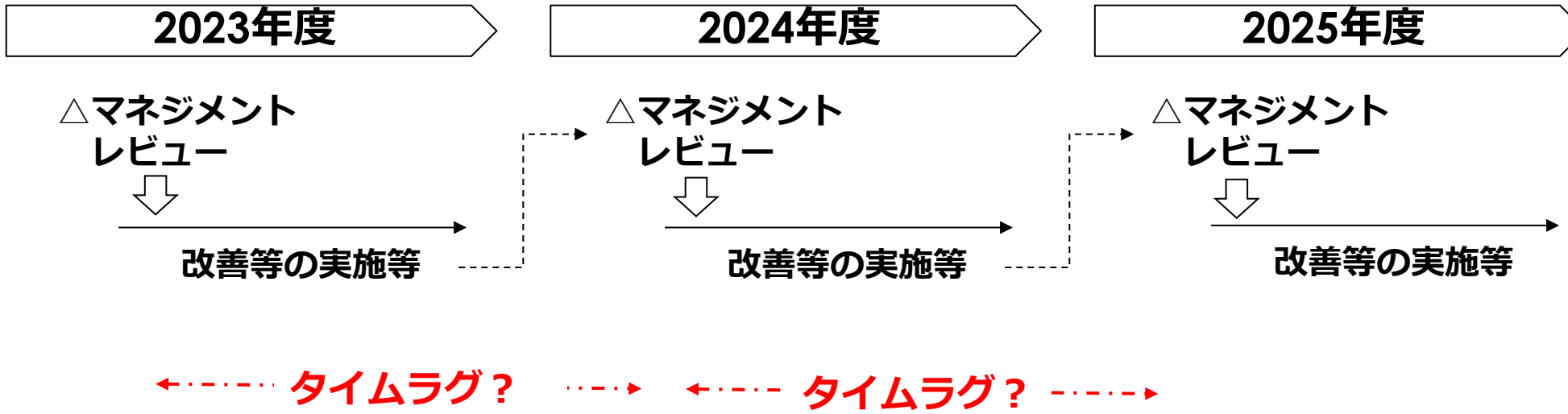
→その結果年1回のイベント的なマネジメントレビューとなっている

問題提起　「セキュリティインシデントは日々発生するのに、経営層の判断が年1回で本当に間に合うのでしょうか？」

事例紹介：マネジメントレビューが年1回の謎について

問題提起

「セキュリティインシデントは日々発生するのに、経営層の判断が年1回で本当に間に合うのでしょうか？」



- 年1回のイベントだと改善のフォローアップが年単位となるため、タイムリーな対応が出来ないと想定されるが、実際の運用実態は？

参考情報

マネジメントレビューの間隔についての考え方　← 規格の本文には明記されていない

○認証機関は「１年を超えない」として審査を実施

例えばISO/IEC 27003（ISMSのための実施の手引き）のガイダンスでマネジメントレビューのあらかじめ定めた間隔について「あらかじめ定めた間隔で、少なくとも1年ごとに見直さなければならない。」と説明

注1：ISOの国際規格の要求事項には、「**あらかじめ定めた間隔で**」実施することが求められているが、**規格の本文に「1年を超えない」という具体的な頻度は明記されていない**

注2：この「1年を超えない」という運用が一般的な背景には、いくつかの要因と、それに関連する文書や慣行がある

1. 外部審査（維持審査）のサイクル

最も大きな理由の一つは、**認証機関による外部審査（維持審査）が通常、年に1回実施されること**

- **維持審査の目的:** 認証機関は、組織のマネジメントシステムが継続的に規格要求事項に適合し、有効に機能しているかを確認するために、年に1回の維持審査（サーベイランス審査）を実施
- **審査準備の必要性:** この維持審査を受けるためには、組織は審査で確認されるべき項目（内部監査の実施、マネジメントレビューの実施、不適合の是正処置など）を事前に完了しておく必要がある
- **実運用上の便宜:** 毎年行われる維持審査に合わせて、その直前や計画的なタイミングで内部監査やマネジメントレビューを実施することが、組織にとって最も効率的かつ合理的な運用となるため

2. マネジメントシステムの継続的改善（PDCAサイクル）

内部監査やマネジメントレビューは、このPDCAサイクルの「Check（点検・評価）」にあたり、**間隔が空きすぎず＆頻繁とならない、1年という期間が適切**とされている

3. 審査機関やコンサルタントの推奨・慣行

参考：マネジメントレビューの運用形態について

マネジメントレビューは年1回に用意周到に準備された会議形態だけでしょうか？

運用形態については様々だが、要件を満たしていればOK

- 飛び込みの1on1mtgでもマネジメントレビューとして成立する
  （但し、記録としてインプット情報、アウトプットとしての指示内容は必要）

- 年1回幹部会議（社長、役員、CISO等）での正式なマネジメントレビューを補完する幹部会議での個別報告＆審議やセキュリティ委員会（CISO、事務局等）での活動がある

  ※：年1回のマネジメントレビューだと適切なタイミング＆鮮度での情報のインプットが出来ないので、普段からの情報共有が大切

- 組織全体の会議対系とISMSの情報のフィードバックループをうまく活用

事例紹介：マネジメントレビューの会議体系について

→ほとんどの組織では年1回のマネジメントレビューの開催となっている（事実）
→多忙な経営層との正式かつ独立したマネジメントレビューは年1回

※：タイムリーな情報共有や相談事項等は下記のような別の会議体、運用形式で実施
※：インプット、アウトプットが明確に記録されれば1on1でもOK

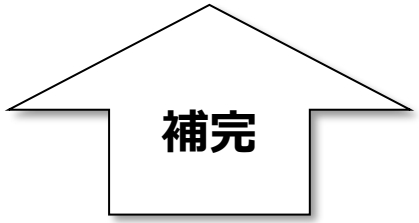
間隔	会議体、付議項目	備　考
日次	日々のモニタリングレポート	日常的なレポートライン
週次	週次のモニタリングレポート	日常的なレポートライン
月次	インシデントレポート	傾向分析含めた組織の健康状態
四半期	セキュリティ委員会	CISO中心としてマネジメントレビューを補完する実務活動
半期	年間計画（予算等リソース審議含む）	マネジメントレビュー相当
年次	トップマネジメントレビュー（総括）	マネジメントレビュー
随時	緊急インシデント対応の相談など突発事項（報連相）	重大インシデントや緊急な経営判断が必要な案件

事例紹介：マネジメントレビューの会議体系について

○○年度 ISMS活動

☆トップマネジメントレビュー（総括）

年1回に集約して実施することで、規格の要件を満たしていることを言明する文書やエビデンスを抜け漏れなく管理することで全体の管理稼働の削減に繋げている



マネジメントレビューを補完する活動支援

審査会社への説明についても資料が分散しなくて都合が良い

△活動計画（年間）

△活動計画（修正）

△セキュリティ委員会（1Q)

△セキュリティ委員会（2Q)

△セキュリティ委員会（3Q)

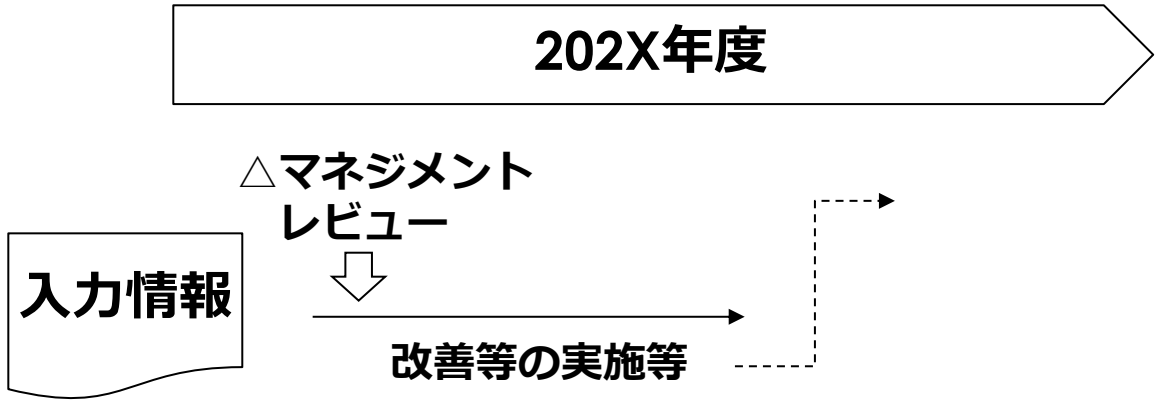
△セキュリティ委員会（4Q)

＋α（随時実施：アドホック会議）

ビジネススタイルの違い（付議時の情報の整理状況の粒度）

パターン1（精緻）

付議までに経営層にGOサインをもらった前提で実施レベルでの**実施項目、課題、コストなどを精緻に資料化**して付議後に実行出来るように準備



ポイント1

精度を上げるための準備期間が必要だが、経営層の判断に必要な情報があり判断しやすい

ポイント2

資料が分散しておらず纏まっているため審査時に提示する資料の管理がらく（網羅性）

パターン2（概略レベル）

方針決定に必要な判断材料を準備

方針決定後に**アジャイル的に詳細化**&実行タスクを作成

フィードバック

事例紹介：マネジメントレビューの付議スタイルの違い

組織の特性や経営層のビジネススタイルに合わせてパターン1（精緻）かパターン2（概略レベル）を選択すべきか変わるが、どちらが正解ということではなく組織の特性に応じて選択すると共に案件によって臨機応変に対応出来るのが望ましいと考える

	パターン1（精緻）	パターン2（概略レベル）
メリット	・詳細なデータが準備されているので判断がしやすい ・マネジメントレビューの要件の網羅性が担保しやすい ・判断後の実行フェーズ移行が早い	・概要レベルなので準備時間が短い ・付議タイミングに即応性がある ・要件の変化に追随しやすい
デメリット	・準備に時間が掛かる ・付議タイミングが遅れる可能性がある ・要件の変化に追随しにくい	・概要レベルでの情報による判断となることから決断しにくい ・情報不足による判断にブレが発生する可能性がある ・マネジメントレビューの要件の網羅性の確認稼働が増える

マネジメントレビューの
インプット情報について

内容＆関連条項
具体的な事例紹介

マネジメントレビューのインプット情報（内容＆関連条項）

インプット項目	内容	関連するISMS活動 / ISO 27001条項
a) 前回までのマネジメントレビューの結果とった処置の状況	前回のレビューで決定された改善活動や指示事項の進捗と結果	マネジメントレビューのアウトプットに対するフォローアップ、継続的改善活動全般
b) ISMSに関連する外部及び内部の課題の変化	事業環境（組織変更、法改正、技術進歩など）の変化とその対応	組織の状況理解（4.1）
c) ISMS に関連する利害関係者のニーズ及び期待の変化	顧客、サプライヤー、株主、規制当局など、ISMSに影響を与える利害関係者からの新たな要求事項や期待を把握	利害関係者のニーズ及び期待の理解（4.2）
d) 情報セキュリティパフォーマンスに関するフィードバック **＜別紙1参照＞**	ISMSの運用状況、有効性、目標達成状況に関する評価結果	不適合及び是正処置 (10.2)、監視、測定、分析及び評価 (9.1)、内部監査 (9.2)、情報セキュリティ目的の達成 (6.2)
e) 利害関係者からのフィードバック	顧客、取引先、従業員などからの情報セキュリティに関する意見や要望	利害関係者のニーズ及び期待の理解 (4.2)
f) リスクアセスメントの結果及びリスク対応計画の状況	最新のリスクアセスメントの結果、新たなリスクの特定、既存リスクの評価、リスク対応計画の実施状況と有効性	リスク及び機会に対処する活動 (6.1)、情報セキュリティリスクアセスメント (6.1.2)、情報セキュリティリスク対応 (6.1.3)
g) 継続的改善の機会	ISMSの運用全体から発見される改善の可能性や提案	ISMSのあらゆる活動（特に「Check」フェーズ全般）

マネジメントレビューのインプット情報（内容＆関連条項）

d）の補足事項

インプット項目	内容	関連するISMS活動 / ISO 27001条項
d）情報セキュリティパフォーマンスに関するフィードバック	ISMSの運用状況、有効性、目標達成状況に関する評価結果	不適合及び是正処置 (10.2)、監視、測定、分析及び評価 (9.1)、内部監査 (9.2)、情報セキュリティ目的の達成 (6.2)
1) 不適合および是正措置	発生した情報セキュリティに関する不適合の内容、是正処置の状況、及びその有効性	不適合及び是正処置（10.2）
2) 監視および測定結果	情報セキュリティ目標の達成状況、ISMSの運用状況に関する監視・測定の結果（例：インシデント発生件数、脆弱性診断結果など）	監視，測定，分析及び評価（9.1）
3) 監査結果	内部監査及び外部監査の結果、指摘事項、改善勧告など	内部監査（9.2）
4) 情報セキュリティ目標の達成	設定された情報セキュリティ目的の達成度合い	情報セキュリティ目的（6.2）

インプット情報として「次の事項を考慮」とは？

ISMSが組織の目標に沿って機能しているか、そして継続的な改善が必要かどうかを判断するための情報

考慮事項	具体例
前回のマネジメントレビューの結果に対する処置の状況	前回レビューで決定された**改善策や是正処置の予実管理（進捗状況＆その結果）**を評価
ISMSに関連する変更	**組織の事業内容、技術、リスク、規制、顧客の要求事項などに変更**があった場合に、ISMSがそれらに適切に対応できているかを検討
ISMSのパフォーマンスと有効性に関するフィードバック	・**インシデント、脆弱性、監査結果、是正処置、監視・測定の結果** ・**利害関係者からのフィードバック**など
リスクアセスメントの結果とリスク処置計画	**新たなリスクや変更されたリスクを評価**し、**それに対する処置計画が適切か**どうかを確認
継続的改善の機会	ISMSをさらに強化するための潜在的な機会を特定（**インプット情報を総合的に分析し、ISMSの現在の状態を正確に把握し、将来の方向性を決定**）

マネジメントレビューへのインプット項目の具体的イメージ

	インプット項目	備考（参考事例）
a)	前回の指示事項等の予実管理	課題管理表、リスク対応計画
b)	組織を取り巻く外部環境（法規制、技術動向、市場の変化など）や、内部環境（組織体制、事業目標、リソースなど）の変化	外部：個人情報保護法改正、AI利用の急速な拡大、 サイバー攻撃の拡大＆多様化など 内部：組織再編成、CSIRT体制の強化など
c)	顧客、サプライヤー、株主、規制当局等の要求事項や期待	預託している個人情報（氏名、住所、クレジット情報）が漏洩しないこと、個人情報保護法やガイドラインに準拠していること
d)	情報セキュリティのパフォーマンスを評価するための様々な指標や活動の結果	不適合の是正処置等、目標達成状況、内部監査結果、目的の達成の進捗状況など
e)	利害関係者（特に顧客）からの意見や苦情、懸念事項	各チャネルを通じて上がってくるクレーム等
f)	新たに特定されたリスク、既存のリスクの再評価、リスク対応計画の実施状況	AI利用拡大による意図しない機密情報の漏洩、サイバー攻撃（新たな脅威情報の共有やランサムウェア感染時のリカバリ対策）など
g)	ISMSの有効性、適合性、妥当性を高めるための改善機会	不適合発生後の対応の有効性の確認＆必要に講じてISMSの変更

参考事例

マネジメントレビューへのインプット項目の具体的イメージ

急激な環境の変化と新たなリスクの認識＆リスク対応

b)	組織を取り巻く外部環境（法規制、技術動向、市場の変化など）や、内部環境（組織体制、事業目標、リソースなど）の変化	**外部：**個人情報保護法改正、**AI利用の急速な拡大、無差別なランサムウェア攻撃の増大**など 内部：組織再編成、CSIRT体制の強化など
f)	新たに特定されたリスク、既存のリスクの再評価、リスク対応計画の実施状況	**AI利用拡大による意図しない機密情報の漏洩、ランサムウェア感染時のコアビジネスの完全停止** **（新たな脅威情報の共有やランサムウェア感染時のリカバリ対策）**など

外部/内部環境の変化

事例1

AI利用の急速な拡大 → **現場サイドでの利用数及び用途の拡大** → **何気なくAIに入力した機密情報の外部流出** → **AI利用に関するルールの制定＆教育の実施**

事例2

無差別なランサムウェア攻撃の増大 → **ウチは重要情報ないので狙われないという根拠のない安心感** → **PCやシステムに感染することでビジネスが長期間停止** → **バックアップの取得＆隔地保管等の対策の実施BCP対策として追加**

マネジメントレビューインプット（事例１）

外部/内部環境の変化

AI利用の急速な拡大（社内/社外）

現場サイドでの利用数及び用途の拡大

AI利用時のリスクについて認識がなく、メリットに目がいく
利用ルール、ガイドラインが未整備

何気なくAIに入力した機密情報の外部流出

社外のAIへ社内の機密情報を入力として答えを求めてしまう

営業秘密情報の漏洩

個人情報の漏洩（お客さま、社員など）

経営層での方針決定

AI利用に関する方針策定

AI利用に関するルールの制定＆教育の実施

- 方針文書
- 社内規定、ガイドライン
- マニュアル
- 研修の実施

投資判断

- 社内専用AI導入
- 社外利用アクセス制限

など

マネジメントレビューインプット（事例２）

外部/内部環境の変化

無差別なランサムウェア攻撃の増大

ウチは重要情報ないので狙われないという根拠のない安心感

無差別攻撃でこれまで狙われなかった組織も無差別に対象となる
利用ルール、ガイドラインが未整備

PCやシステムに感染することでビジネスが長期間停止

情報セキュリティの脅威

JISQ27001:2023で新規追加された 5.7脅威インテリジェンスとの連携

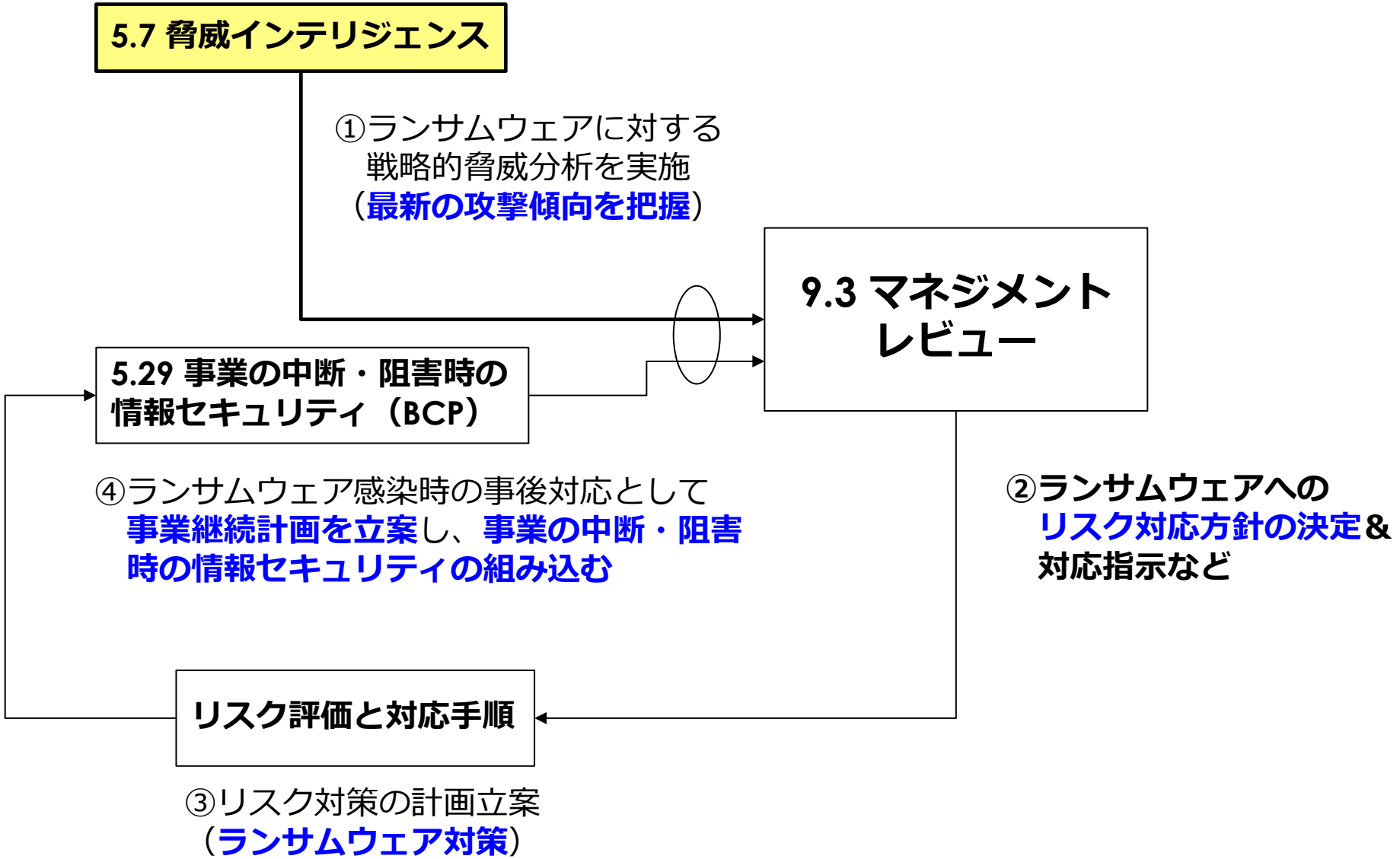
脅威インテリジェンスからのアプローチ

情報セキュリティの**脅威に関する情報を収集及び分析し、脅威インテリジェンスを構築**することが求められているので、
箇条5.7の活動結果をインプットとして
情報を整理してインプットする

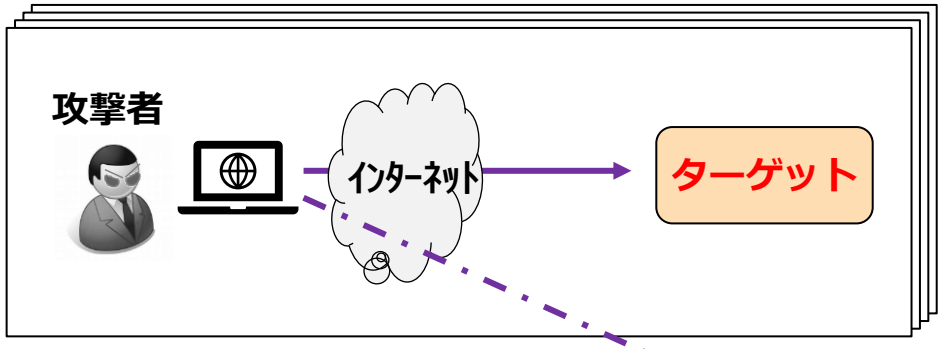
戦略情報として判断に必要な情報

- ランサムウェアの脅威度
- 自組織での対応状況
- 発生時のビジネスインパクト

ランサムウェア対策とマネジメントレビュー



5.7 脅威インテリジェンス（イメージ図）



サイバーセキュリティの
専門家が分析・整理した
サイバー攻撃に関する
情報を収集

外部組織

専門組織

セキュリティ研究機関、
NPO法人、セキュリティ
ベンダー、など

サイバー攻撃に関する情報

- 攻撃のメカニズム（攻撃手法）
- 攻撃の発生の識別方法
- 攻撃によってビジネスに与える影響
- 防御方法などのアドバイス

マネジメントレビュー
のインプット情報

内部組織

防御

戦略情報として
のインプット

マネジメント層
主要な意思決定者、
CEO、取締役など

セキュリティ担当
セキュリティ技術者
CSIRTやISMS事務局

IT部門
ITシステムの開発＆
運用部門

攻撃に対する防御情報
としてのインプット

ランサムウェアに対する脅威インテリジェンスの活用

ランサムウェアは、管理策5.7が特に対処すべき**最も重大で変化の激しい脅威**の一つです。
脅威インテリジェンスは、ランサムウェア攻撃から組織を防御するために不可欠な情報源

脅威インテリジェンスの活用	ランサムウェア対策への具体的な貢献
攻撃手法の把握	新しいランサムウェアの亜種や、マルウェアの侵入・拡散経路（例えば、特定の脆弱性の悪用、フィッシングメールの手口など）に関する情報を収集し、**防御策を先取り**する。
攻撃者の特定と動向	攻撃グループの目的、標的とする産業、使用するツールや戦術（TTPs*1）を把握することで、**自組織が標的になるリスクを評価**し、それに基づいたセキュリティ対策（例：多要素認証の導入強化）を優先的に講じる。
検知・対応の強化	ランサムウェアのC2サーバーのIPアドレスやファイルハッシュなどの技術的指標（IoC）をセキュリティ監視ツール（SIEM、EDRなど）に取り込み、**攻撃の初期段階での検知能力を向上**させる。
リスクアセスメントへの反映	最新のランサムウェアの傾向を**リスクアセスメントのインプット**とし、ランサムウェアによる事業継続への影響（データ損失、システム停止など）を評価し、**バックアップ戦略**や**復旧手順**を最適化する。

*1：Tactics, Techniques, and Procedures

規格要求事項と戦略インテリジェンスの関連性

規格要求事項への貢献	戦略インテリジェンスの焦点
リスクアセスメントのインプット	自組織の**業種**や**地理的状況**を標的とする**ランサムウェアグループの動向、攻撃の成功率、身代金の平均額、およびデータ漏洩の傾向**
経営資源の配分	ランサムウェア攻撃の**影響度（事業継続性への影響）の評価に基づき、予防策（例：EDR導入、バックアップシステムの強化）と復旧策に割くべき予算、人材、時間**の優先順位付け
セキュリティ戦略の策定	ランサムウェア攻撃者の**TTPs（戦術・技術・手順）の長期的な変化傾向を把握し、向こう数年間にわたり組織の防御能力をどこまで高めるべきか**を決定

2. ランサムウェアに関する戦略インテリジェンスの具体的な内容

戦略インテリジェンスは、ランサムウェアという脅威全体を俯瞰し、
「なぜ、誰に、どれだけ投資すべきか」を判断するために用いる

戦略インテリジェンスの要素	ランサムウェア対策への活用
攻撃者のプロファイル	**RaaS（Ransomware-as-a-Service）モデルの普及状況、主要な攻撃グループ（例：LockBit, BlackCat）の活動地域、標的とするシステムの脆弱性のトレンド** 経営層は、これらの情報から**攻撃リスクの増減を判断**
規制・法的影響	ランサムウェアによる**個人情報漏洩が発生した場合の各国の規制**（例：GDPR, CCPA）や**業界の法令遵守（コンプライアンス）上の義務** これに基づき、インシデント対応計画や情報公開ポリシーを策定
インシデントコスト	実際に攻撃を受けた企業の**身代金支払い**の有無、**復旧にかかった時間と費用**、**株価への影響**など、金銭的・非金銭的な総合的被害データ **セキュリティ対策への投資対効果（ROI）を経営層に説明する根拠**
技術的ロードマップ	攻撃者が次に狙うと予測される技術（例：クラウド環境、OTシステムなど）に関する情報 組織の**セキュリティ技術導入計画や従業員の教育内容の方向性**を決定

参考資料

情報セキュリティマネジメントセミナー2023（講演資料）

規格要求事項から見た整理

5.7 脅威インテリジェンス

このテーマの中では、人的、組織的、物理的、技術的の4つの分野の脅威の中から、変化が激しく組織に重大な影響を与える可能性の高いサイバーセキュリティの脅威を「脅威インテリジェンス」の研究対象として取り上げます

5.7 脅威インテリジェンス（要約）

概要

情報セキュリティの脅威に関する情報を収集及び分析し、脅威インテリジェンスを構築すること。

実現したいこと

サイバーセキュリティの脅威（※1）から組織の活動を守るため、脅威インテリジェンスを活用する

※1：このテーマの中では、人的、組織的、物理的、技術的の4つの分野の脅威の中から、変化が激しく組織に重大な影響を与える可能性の高いサイバーセキュリティの脅威を「脅威インテリジェンス」の研究対象とする

具体的な対応内容や補足事項など

・脅威インテリジェンスは、攻撃者の動機、標的、攻撃手法を理解して対応するために収集・分析されたデータ

・経営戦略的な判断をするための入力情報として活用（経営層）したり、予想される攻撃や実際の攻撃から防御する　ための入力情報として活用（セキュリティの専門家、システム担当など）

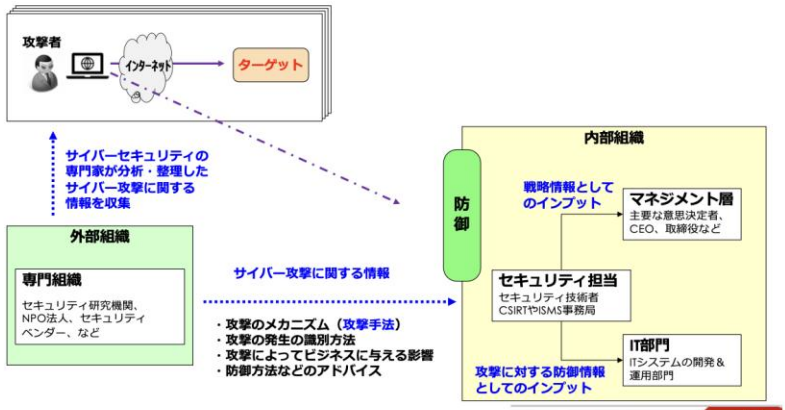
<情報の例示>
サイバーセキュリティの専門家が分析・整理したサイバー攻撃に関する情報

・攻撃のメカニズム（攻撃手法）
・攻撃の発生の識別方法
・攻撃によってビジネスに与える影響
・防御方法などのアドバイス
・攻撃を実現させる環境・条件があるか

抜粋版

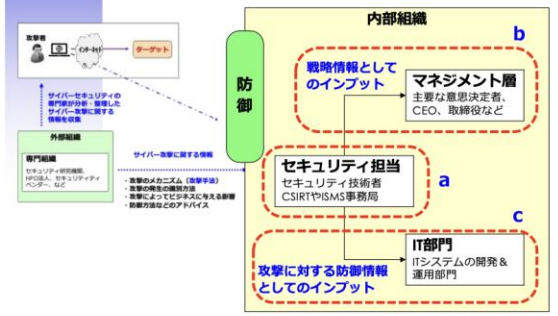
https://www.jnsa.org/result/isms/seminar/2023/2023-003.pdf

5.7 脅威インテリジェンス（イメージ図）



脅威インテリジェンスの活用ポイント・・・a、b、c

専門機関からの収集する情報を整理してサイバー攻撃に対する防御に有効活用するプロセスを確立する



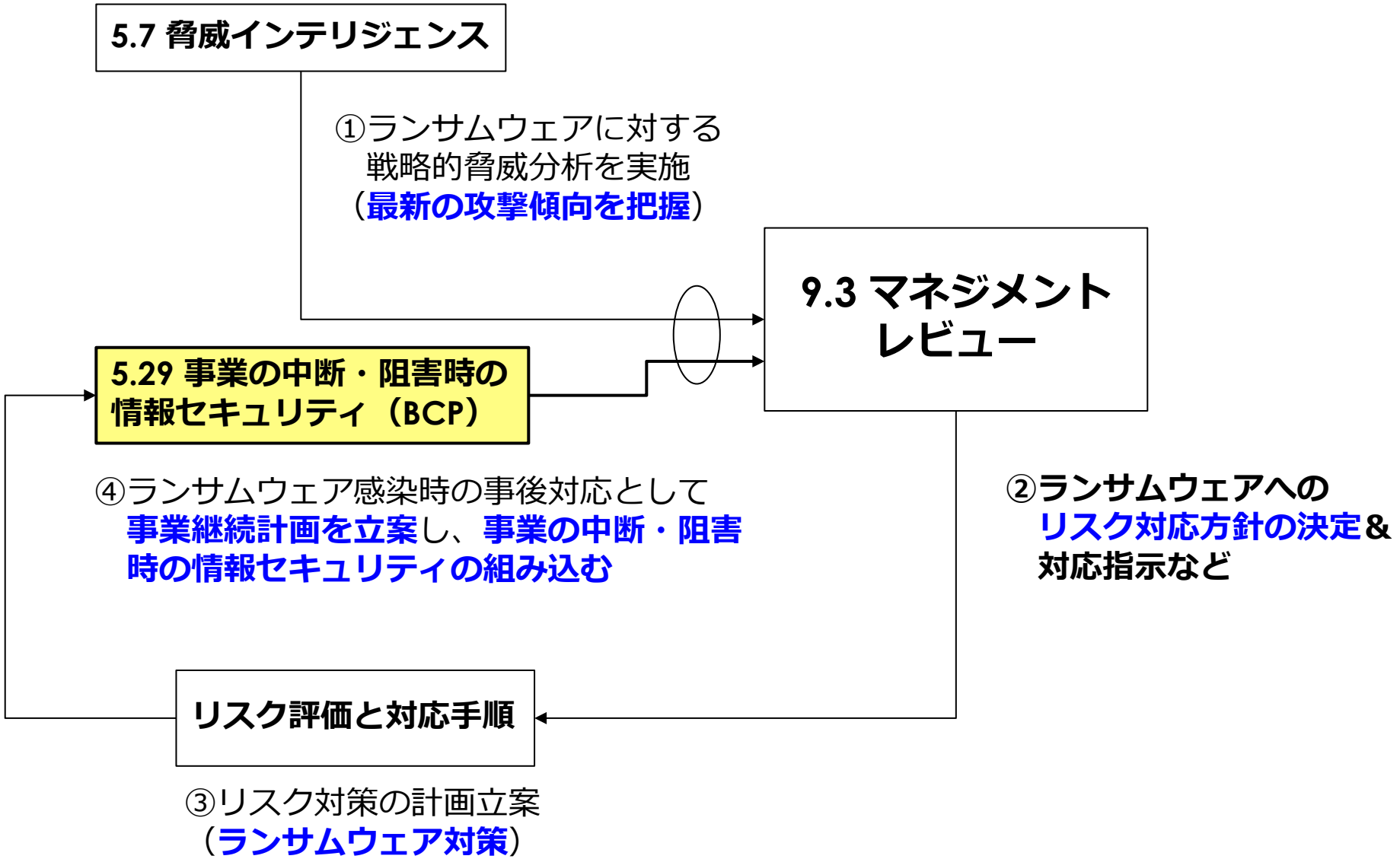
活用ポイント

a.脅威情報を簡易分析（判断）する機能を実装し、情報を伝達する

b.経営層へのインプットする条件やタイミングの判断基準を作成

c.関係部署（社員、システム担当）に流す情報と期待する行動を定義する

ランサムウェア対策とマネジメントレビュー



感染前提の事後対策について点検＆情報共有を忘れずに！

予防保全

＋

事後対策

5.30 事業継続のための ICTの備え

感染前提の準備を
忘れずに！

・最重要ビジネスの絞込み
・システムのバックアップ＆保全
・リカバリプランの再確認
（RTO/RLO）

感染前提の事後対策について点検＆情報共有を忘れずに！

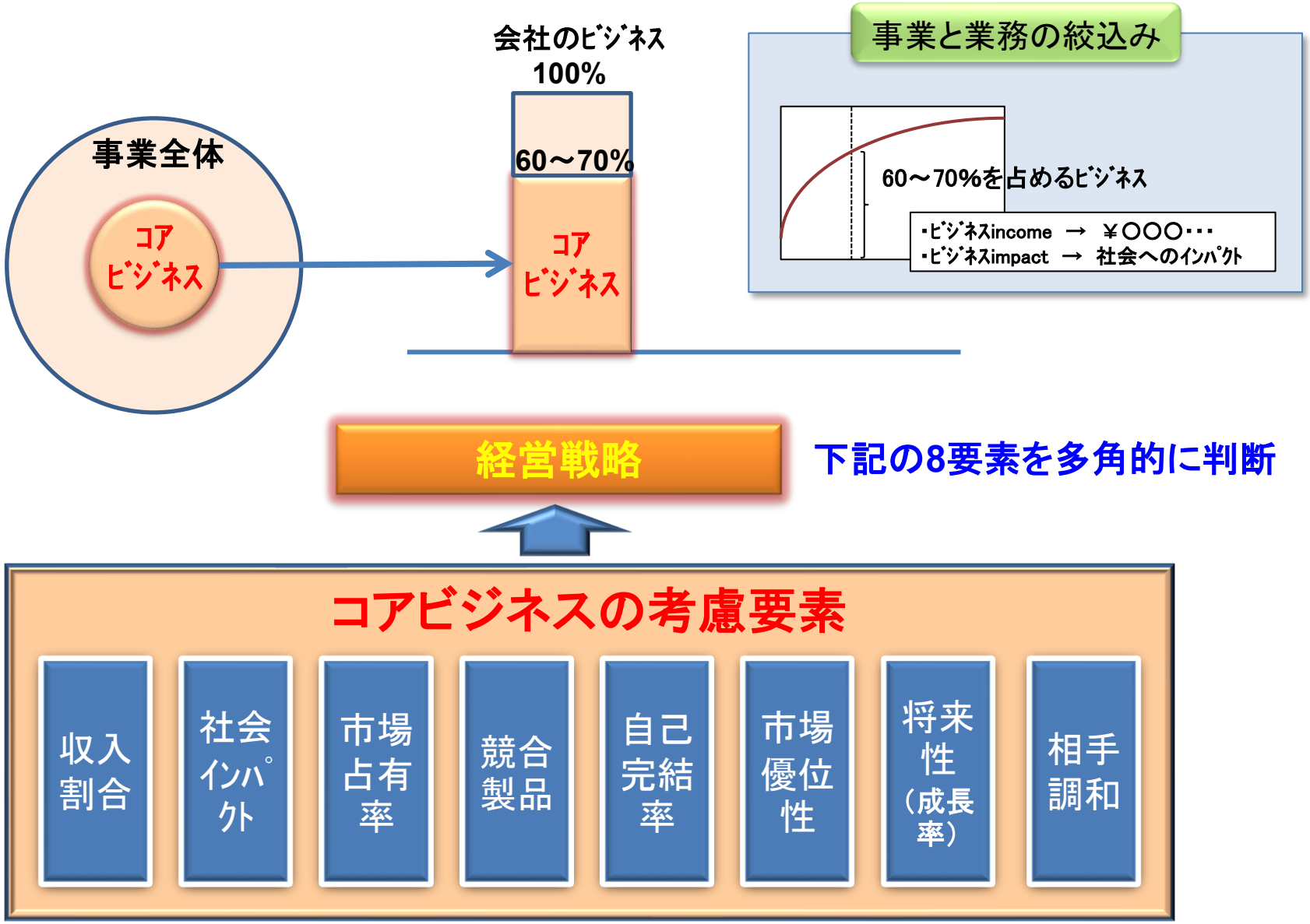
経営層へのインプット情報

①ランサムウェア感染時のビジネスインパクト
（コアシステムが感染した場合の影響範囲）
・サービス停止想定期間
（感染～分析～リカバリ）
・影響するビジネス規模（損失費用）

②BCP対応状況
・コアビジネスの絞込み
・コアシステムの対応状況
-バックアップ＆メディアの隔離＆保護
-リカバリ手順作成＆検証
・その他システムの対応状況
-システム間連携時には感染拡大

参考資料

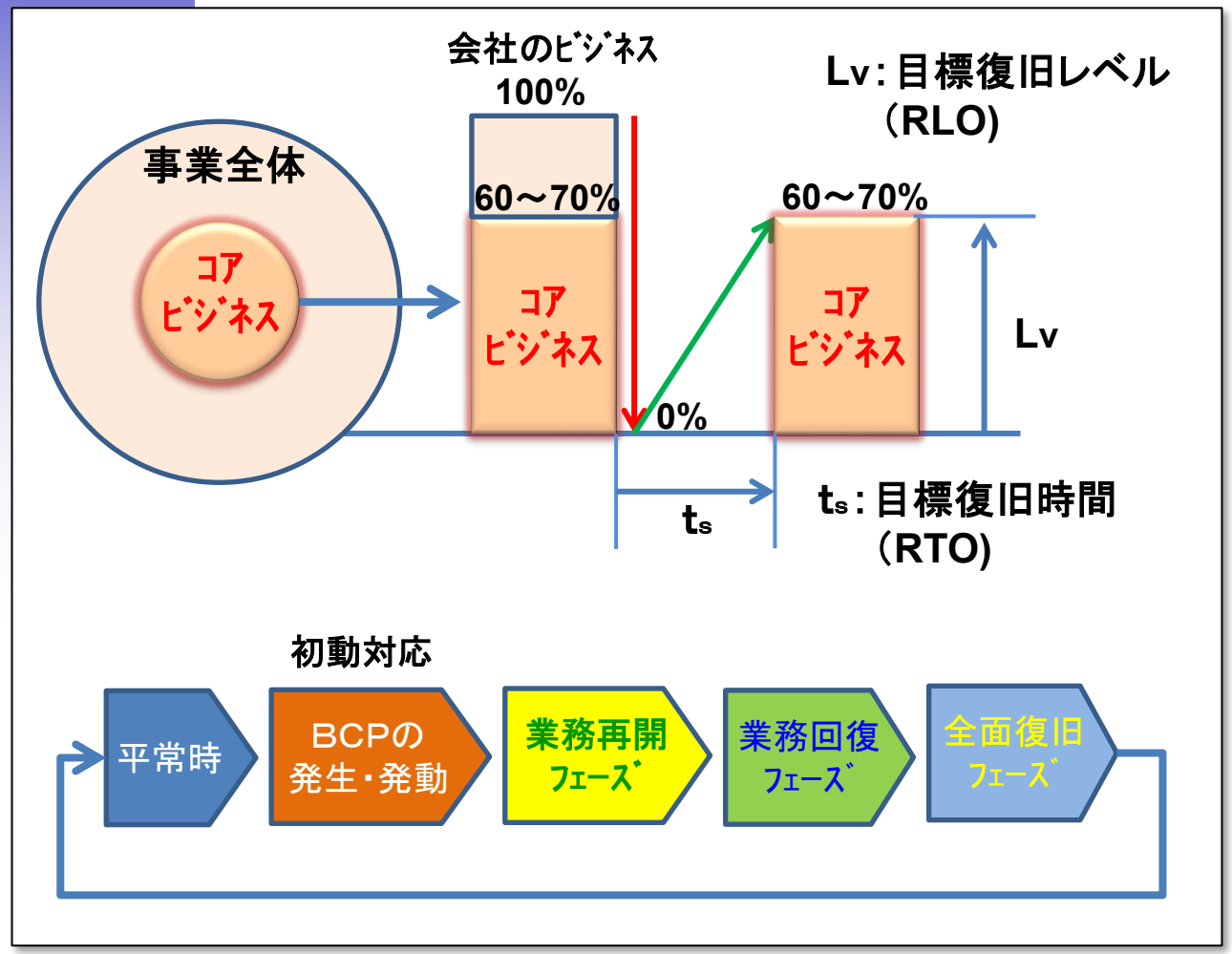
コアビジネスの考慮要素と絞込み



参考資料

コアビジネスの目標復旧レベル（RLO)と目標復旧時間（RTO)

事業継続計画



5.30 事業継続のための ICTの備え

要素を加味

災害発生やサイバー攻撃などの緊急時において業務に必要なICTシステムを維持する

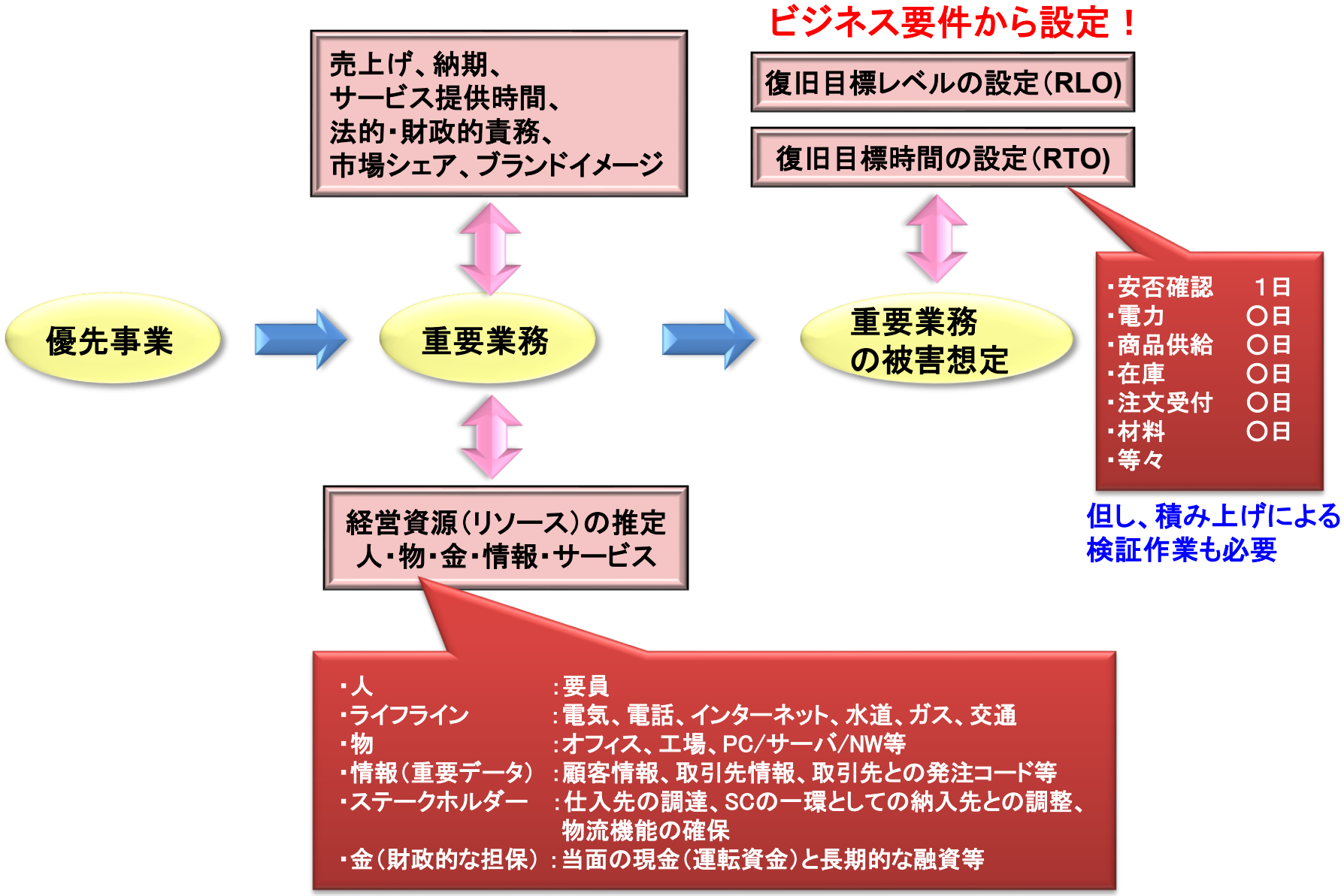
整理の観点

- ICTと業務との関係性
- ICTの管理責任者の明確化
- ICTの課題とその対応策
  （データ保管＆バックアップ、リモートワーク、コミュニケーション手段、セキュリティ対策など）
- BCP時のICT復旧の見込みや対策

など

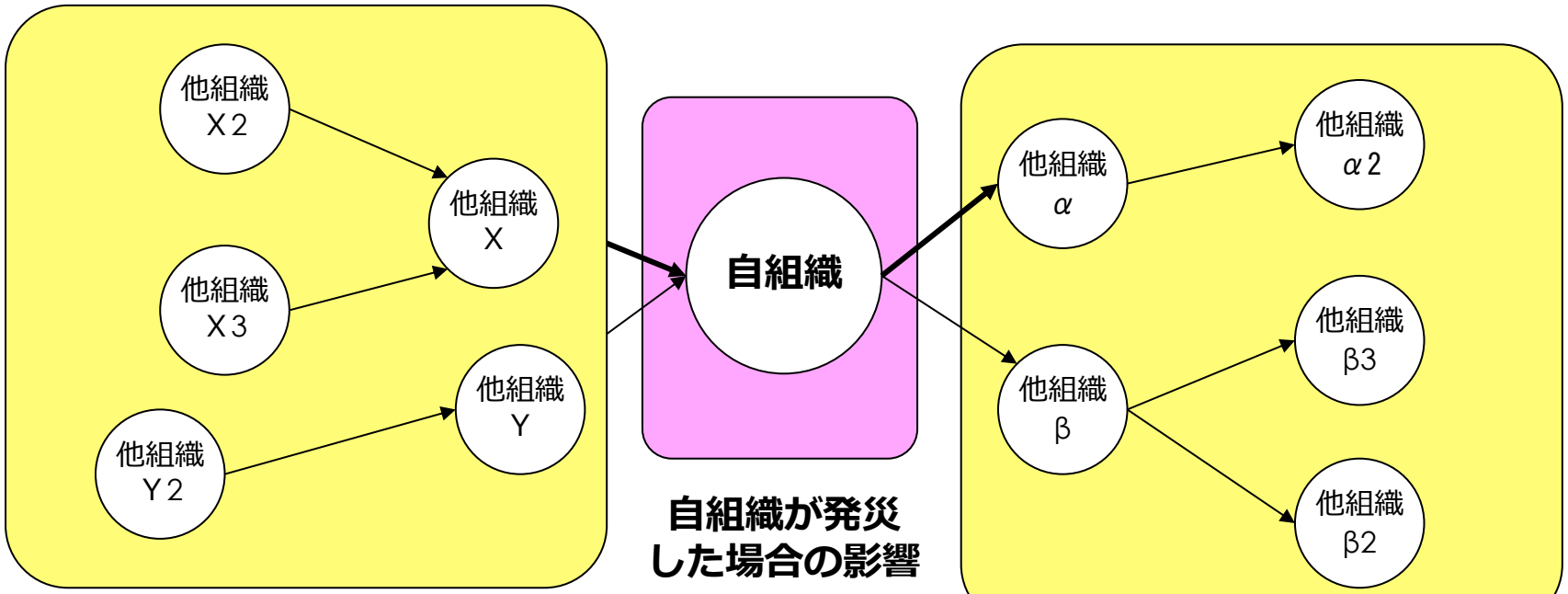
参考資料

BCP対象業務の絞り込みの考え方



ランサムウェア感染時のビジネスへの影響範囲と考慮事項について

- 自組織だけでなく、関連するステークホルダーの関係についても事前に整理が必要
- 自組織のサービスが停止した場合の損失や関連するステークホルダーへ与える影響など対策案の机上検討や連絡ルートの整備など



関連ステークホルダが発災した場合の自社への影響

自組織が発災した場合の影響

自組織が発災した場合の関連ステークホルダへ与える影響

マネジメントレビューインプット（事例２）

外部/内部環境の変化

無差別なランサムウェア攻撃の増大

ウチは重要情報ないので狙われないという根拠のない安心感

無差別攻撃でこれまで狙われなかった組織も無差別に対象となる
利用ルール、ガイドラインが未整備

PCやシステムに感染することでビジネスが長期間停止

現在のビジネスはIT無しでは成り立たない状況なのでBCPの観点での検討が必要

PCやシステムへの侵入対策

バックアップの保護

経営層での方針決定

ランサムウェアに関する方針策定

感染しないための予防保全
＋
BCP対策として追加し、リカバリプランを検討

- 方針文書
- 社内規定、ガイドライン
- マニュアル
- 研修の実施

投資判断

- 社内システムの現状調査
- 隔地保管などバックアップ＆リカバリ計画の策定

マネジメントレビューの
アウトプット情報について

アウトプット情報
とその影響

マネジメントレビューのアウトプット情報とその影響

アウトプット項目	内容	その後のISMS活動への影響
1) 改善の機会	ISMSの**有効性向上に向けた具体的な改善点、推奨事項、新たな取り組み**の決定	特定された問題に対する改善策の導入、ISMS改善計画の策定と実行、次期PDCAサイクルの「Plan」へのフィードバック
2) ISMSのあらゆる変更の必要性	**情報セキュリティ方針、目的、リスクアセスメント基準、組織構造**など、ISMS構成要素の変更に関する決定	ISMSの設計・運用に関する変更計画の策定と実施、情報セキュリティ方針・目的の見直し、組織の戦略的変化へのISMSの適応

文書化*1

1）と 2）について文書化する

1）と 2）を確実に実行するために必要なリソースを明記＆担保

＊1：補足事項

ISMSの運用・維持・改善に必要な人的、物的、財政的リソースに関する決定

例）必要なリソースの確保、教育訓練計画の策定と実施、従業員の意識向上、予算配分、技術的リソースの導入・更新

マネジメントレビューのアウトプットと具体的なISMS活動への影響

マネジメントレビューのアウトプット内容及び具体的なISMS活動への影響

	内容	その後のISMS活動への影響
①	**リスク対応計画の更新**	**新たに特定されたリスクや既存リスクの変化**、またはリスク対応策の有効性評価に基づき、**リスク対応計画を更新**
②	**情報セキュリティ方針・目的の見直し**	**組織の状況変化、利害関係者からのフィードバック、パフォーマンス評価の結果**に基づき、**情報セキュリティ方針や目的の調整または改訂**
③	**リソース配分**	決定された資源の必要性に基づき、**情報セキュリティ関連の予算、人員配置、技術的リソースの導入・更新の計画・実行**
④	**教育訓練計画の策定・見直し**	**力量不足の解消、新たな脅威への対応**、または特定の管理策の強化のために、**教育訓練計画が策定または見直し**
⑤	**内部監査計画の調整**	マネジメントレビューで指摘された改善の機会や変更の必要性に応じて、**次期の内部監査の重点領域や範囲の調整**
⑥	**文書化された情報の維持**	**マネジメントレビューの結果、決定事項**、および**それに基づく処置内容**は、ISMSの記録として適切に文書化され、保管されます

有効なマネジメントレビュー
を目指して・・・

有効なマネジメントレビューの実現のためには・・・

・トップマネジメントの積極的な参加

・情報セキュリティパフォーマンスの透明な議論

・明確な意思決定

単に規制や認証要件を満たすことにとどまらず、**組織に具体的な価値を生み出す**ことにフォーカスするには、**目的や判断ポイントの明確化と決定事項の確実な実行**プロセスに繋げることが重要！

※：形式的なプロセスについては形骸化しやすいリスクが内在しやすい

マネジメントレビューの様々な課題に対する考慮事項

形式的な実施とならないためには・・・

・**インプット情報の質と量（良質なインプット情報）**

- レビューのインプットが**不足**、**不正確で適切に判断出来ない**
- 情報が多すぎると、**重要な点を見落とす**

・**アウトプットの実行力（予実管理＆フォローアップ）**

- レビューで決定した**改善策や必要な資源の提供**といったアウトプットが、**実際には実行されない**、または**遅延することを防止**
- 資源の確保や組織横断的な変更に関わる決定事項は、**トップマネジメントの強いフォローアップ**が必要

・**トップマネジメントのセキュリティへの理解（組織を取り巻く状況の理解）**

- 情報セキュリティを**コスト**ではなく**投資**や**ビジネス上の優位性**として理解

日頃からのコミュニケーションが重要

・お互いに声掛け

・話題の提供（ランサムウェア、AIなど最新の脅威を題材にして）

・自組織の立ち位置（Green、Yellow、Red)について

・ビジネスインパクトの共有

・ネガティブな面（記者会見を想定）にもフォーカスを

・責めないでリスクの可視化と改善ポイントを中心に

・アジャイル的に

マネジメントレビューのベストプラクティスの提案

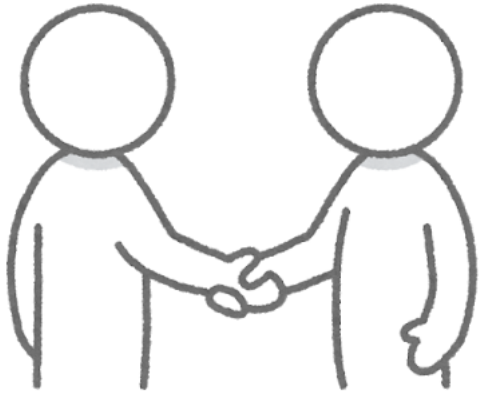
推奨事項	備考・補足事項
明確な目的設定とアジェンダ作成	下記を盛り込んだアジェンダ作成 **・目的の明確化** **・目的に達成に必要なインプットと期待されるアウトプット** ※：要求事項に合わせたチェックシートの活用による網羅性の担保
正確かつタイムリーなインプット情報の収集	・ISMSの各活動（内部監査、監視測定、リスクアセスメントなど）のデータを**正確かつ良質な情報をタイムリーに集約** ・経営層向けに**適切は粒度でのサマライズ**した資料
トップマネジメントの積極的な関与	レビューの有効性を最大限に引き出す ために積極的に参画 ・経営層が情報セキュリティに関する**リスクや運用状況を見極め（組織を取り巻く状況の理解）、戦略的な意思決定を行う唯一の場であることを認識** ・トップマネジメントが**率先して指揮統率し、議論に積極的に参加**
具体的かつ実行可能なアウトプットの決定	決定事項は、**具体的な処置内容、担当者、期限を明確**にする ※：決定を確実に次のISMS活動に繋げ、形骸化を防ぐ
決定事項の確実なフォローアップ	アクションプランの実施状況は、**継続的に予実管理＆フォローアップ**する ※：フォローアップの結果は、次回のマネジメントレビューの重要なインプット
組織の方針との整合性	アウトプットは、組織の全体的な**事業戦略や組織の方針と密接に整合**しているか？ ※：組織の方針に照らし合わせながらアウトプットを行う
定期的な実施	ISO 27001の要求事項に基づき、マネジメントレビューは少なくとも年に1回は実施 ※：**定期的な実施**は、ISMSの継続的な監視と改善に不可欠

まとめ

年1回のトップマネジメントレビューに加えて最新の環境の変化（AIやランサムウェア）についてビジネスリスクと組織の置かれた状況についてディスカッションから始めてみませんか？
経営層やCISO、ISMS事務局共に新たな気づきや発見が生まれるはずです

- 適切な頻度での開催（年1回＋α）
- 経営的判断が可能な情報の粒度でのインプット
- マネジメントレビューの目的
  （中長期的な視点での判断＆改善指示）
- 透明性（良いデータも悪いデータも等しく開示）
- 自組織だけでなく取り巻く社外環境含めて判断
- 良質な相互コミュニケーション

相互理解



参考資料

参考資料

情報セキュリティ定期報告【報告】案　（参考事例）

20XX年度 第4四半期の情報セキュリティ インシデント発生状況等について、ご報告致します。

1．【報告】情報セキュリティ インシデント発生状況（20XX年度 第4四半期）

2．【報告・依頼】20XX年度 情報セキュリティ インシデント・ヒヤリハット発生状況

3．【報告】20XX年度 情報セキュリティ定期研修実施結果

4．【報告】20XX年度 標的型攻撃メール対策訓練実施結果

5．【報告】プライバシーマーク更新審査の受審結果

6．【報告】情報セキュリティ自治点検結果（20XX年度 第4四半期）

7．【報告】お客様個人情報に関する運用確認結果

8．【報告・依頼】XXグループ 情報セキュリティ・システム監査結果

9．【報告・再依頼】 EDR導入、検疫環境利用について

10．【周知・依頼】 その他周知事項

出席者：社長、役員（本部長）、事務局
陪席者：監査役、副本部長、関係スタッフ部門

参考資料

セキュリティ委員会付議事項案　（参考事例）

情報セキュリティ委員会の審議内容には、以下に掲げるような内容を含こと　（規格要求事項を参考）

情報セキュリティ年間計画（年間セキュリティ教育計画、及び年間情報セキュリティ監査計画を含む）（年一回付議）
ISMSにおける監査結果報告及びその問題点、改善点について
外部監査結果報告及びその問題点、改善点について
ISMSの運用状況
利害関係者からの要求事項への対応について
事業領域、及び組織の変更への対応について
適用規格の要求事項の変更への対応について
関連法規制の改正状況への対応について
是正措置について（必要性、計画、進捗・結果報告に対するフォローアップ等）
リスク対応計画の更新について
有効性測定結果報告及びその問題点、改善点について
苦情を含む外部からの意見
内外から寄せられた改善のための提案
社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化
その他、大規模投資案件、インシデント報告、問題点、及びその対応等について情報セキュリティ責任者（CISO）が判断した報告・審議案件

経営陣による改善指示は、以下に掲げるような決定及び処置を含む。

ISMSの有効性の改善についての決定事項
リスクアセスメント及びリスク対応計画の更新についての決定事項
必要な経営資源についての決定事項
管理策の有効性測定方法の改善についての決定事項
その他の修正事項、事業上の要求事項、情報セキュリティ要求事項、既存の事業上の要求事項を満たす業務プロセス、規制環境または法的環境、契約上の義務、リスクの水準及びリスクを受容するための基準についての決定事項

参考資料

幹部会議＆セキュリティ委員会付議実績　（参考事例）

年度	日付	幹部会議 ○規程改定 ●インシデント報告	セキュリティ委員会	内容
20XX年度	4月	○		情報セキュリティ個別規程制定
	6月		○	セキュリティ関連情報/内部監査・外部審査（計画付議）
	8月		○	「情報セキュリティ委員会」体制等の見直し/内部監査報告
	9月		○	外部審査報告/内部監査・外部審査の結果対応課題
	11月	○		トピック（マイナンバー対応：方針＆運用）
	12月	○		（上記にかかわる規程修正）
	12月		○	トピック（パートナー社員等の情報管理プロセス適正化）
	1月	○		（上記にかかわる規程修正）
20XX年度	4月	●		3月分インシデント報告
	5月		○	年間スケジュール
	5月	●		4月分インシデント報告
	6月		○	内部監査（計画付議）
	6月	●		5月分インシデント報告
	7月	○		ＢＣＰ（災害対策規程改定他）
	7月	●		6月分インシデント報告
	8月		○	内部監査報告・外部審査実施
	9月		○	「情報セキュリティ内部監査・外部審査」結果に対する20XX年度下期の対応方針等について

参考資料

ISMS年間活動計画表（例）