日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA 2026年度活動報告会

日本ISMSユーザグループ

「標準化動向やインプリメンテーション研究会の活動の情報発信など」

標準化部会　日本ISMSユーザグループ

WGリーダー　魚脇 雅晴

（NTTドコモビジネス株式会社）

2026年7月22日

本日の説明の流れ

1. ISMS-UGの紹介

・標準化部会とISMS-UG
・ISMS-UGの活動（標準化と研究会との関係）

2. 2025年の活動報告

・標準化動向（27000ファミリー規格最新動向＆27017ポイント解説）
・インプリメンテーション研究会の活動（マネジメントレビュー ）抜粋

3. 2026年の活動計画案

・インプリメンテーション研究会の活動（ホットな話題４テーマ）
・情報セキュリティマネジメントセミナーのご案内（12/4）
・LT形式の勉強会のご案内（9/15）

4. インプリメンテーション研究会へのお誘い

日本ISMSユーザグループのご紹介

標準化部会のWG　日本ISMSユーザグループ

**業種・業界・分野等の標準化・ガイドライン化などを推進する。
特にJNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメント、国際連携案件も視野に入れて、議論を進める。さらに、近年のデジタル化促進にともなる技術要素についても積極的に取り上げ、標準化部会での技術共有や課題抽出を実施していく。**

- **デジタルアイデンティティWG**
- **電子署名WG**
- **日本ISMSユーザグループ**
- **PKI・PQC運用技術WG**

https://www.jnsa.org/active/std.html

日本ISMSユーザグループの活動目的＆予定

１．WGの活動目的

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで
ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における
健全かつ効果的なISMS普及・促進に貢献する活動を行う

２．WGの年間活動予定

- **インプリメンテーション研究会におけるISMSの構築や運用における課題検討（毎月）**
  （メインテーマとして「新規格改定に伴う新規管理策の実装方法について」検討を行う）

- **情報セキュリティマネジメントセミナーの開催と研究結果の発表（12月）**
- **LT（ライトニングトーク）形式勉強会の開催（9月）**

日本ISMSユーザグループの活動紹介

標準化動向

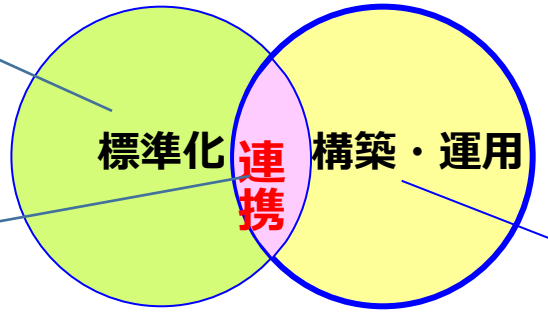
標準化の活用＆定着

ISMSの普及・促進

情報セキュリティ
マネジメントセミナー

標準化動向
の情報発信

貢献



リエゾン参加

SC 27/WG1 小委員会
アドホック会議

インプリメンテーション研究会

ISMSの構築・運用におけるベスト
プラクティクスを検討＆提供

標準化されたものをどのように
ビジネスの世界に反映＆定着
させるか・・・

インプリメンテーション研究会の活動紹介

2006年～　ISMSの構築・運用におけるベストプラクティスを検討＆提供　現在

【過去のテーマ名】（2015年以前は省略）

2021年 ■ISMSとゼロトラストセキュリティについての考察
■ISMS要求事項の解釈と運用の実態

2020年 ■実践かつ効果的なセキュリティ教育
■規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み

2019年 ■最新の環境変化に伴うISMSの実装検討
■各社の事例から学ぶISMSの実装について

2018年 ■ISMS規格要求事項から紐解く最新のビジネス環境リスク
■働き方改革における情報セキュリティ

2017年 ■現場と連携したリスクアセスメント手法の実践活用
■内部監査を有効に運用するための手法の考察

2016年 ■サイバー攻撃を事例としたリスクマネジメントの実践
■運用フェーズにおける有効性の評価

2026年

■キャリアパス
■AI活用実践（応用）
■規格要求事項から見たランサムウェア対策状況の可視化
■AI活用実践（入門）

本日ご紹介

2025年

■ なぜ話が通じない？ ISMS審査・運用の現場で起こる認識のズレ
■ 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
■ 生成AIで進化する、次世代のISMS運用の形

2024年 ■ JISQ27001:2023の新規管理策の実装方法についての考察
■ ISMS内部監査どうやってますか?

2023年 ■ JISQ27001:2023の新規管理策の実装方法についての考察
■ ISMS内部監査どうやってますか?

2022年 ■最新の環境の変化に対応したISMSのスコープの再定義について
■続・効率的リスクアセスメント

2025年の活動実績

■情報セキュリティマネジメントセミナー2025

（27000シリーズの最新動向とベストプラクティスの提案）　2025年12月5日（金）PM

JNSA

標準化動向

ISO27001、ISO27002などの27000シリーズの標準化の最新動向など

- 「ISO/IEC 27000ファミリー規格 最新動向」
- 「ISO/IEC 27017 ポイント解説」

研究会活動成果

インプリメンテーション研究会の活動成果

テーマ1：「なぜ話が通じない？ ISMS審査・運用の現場で起こる認識のズレ」

テーマ2：「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」

テーマ3：「生成AIで進化する、次世代のISMS運用の形」

【パネルディスカッション】最新のトピック（形骸化＆AI）についてディスカッション

テーマ1：「形骸化」の壁をどう乗り越えるか？ ～現場と経営、ルールと実態のズレをなくす処方箋～

テーマ2：AIはISMS担当者を救うのか？ ～テクノロジーが変える情報セキュリティマネジメントの未来図～

講演映像　講演映像をYouTube JNSAChannelで公開中＞＞ JNSA CHANNEL

https://www.youtube.com/playlist?list=PL1nvarmw8MRuw4IrQ1TTTo7vRqz8Oe6XR

講演資料　https://www.jnsa.org/seminar/std/isms/20251205/index.html

詳細についてはこちらを参照

標準化動向

- 「ISO/IEC 27000ファミリー規格 最新動向」
- 「ISO/IEC 27017 ポイント解説」

「ISO/IEC 27000ファミリー規格 最新動向」

（概要）

ISO/IEC 27001（ISMS－要求事項）とISO/IEC 27002（情報セキュリティ管理策）の2022年の改訂を受けて、現在ISO/IEC 27000（ISMSの用語及び手引）やISO/IEC27003（ISMSの手引）などの各種ISO/IEC 27000関連規格の改訂が順次進められています。本講演では、これらの主要なISO/IECファミリー関連規格の最新動向について概観します。

ポイント：改訂が進む関連規格の全体像と最新トレンドの把握

2022年の「ISO/IEC 27001（要求事項）」および「ISO/IEC 27002（管理策）」の改訂に伴い、用語や手引を定めた「27000」「27003」など、他のファミリー規格も順次改訂が進められています。これら主要規格の最新動向を俯瞰することで、今後のISMS運用の道標を示しています。

「ISO/IEC 27017 ポイント解説」

（概要）

現在、クラウドセキュリティのガイドライン規格であるISO/IEC 27017が改訂されようとしています。ISO/IEC 27017のベースとなっているISO/IEC 27002（情報セキュリティ管理策）においては、2013年版では「クラウドサービス」への言及はありませんでしたが、2022年版では「5.23クラウドサービスの利用における情報セキュリティ」の管理策をはじめとして、その他の管理策の手引においても数多くの「クラウドサービス」への言及があります。本講演では、ISO/IEC27002:2022におけるクラウドサービスに関する情報セキュリティ管理策や手引と、ISO/IEC 27017におけるクラウド固有の管理策や手引の関係を整理し、ISO/IEC 27017の理解を深めるためのポイントを解説します。

ポイント：新旧規格における「クラウドセキュリティ管理策」の整理と理解

改訂を控えるクラウドセキュリティのガイドライン規格「ISO/IEC 27017」に焦点を当てています。ベースとなる「ISO/IEC 27002:2022」で大幅に強化されたクラウドサービスに関する記述（管理策5.23など）を踏まえ、両規格の相関関係を整理し、クラウド固有のセキュリティ管理を深く理解するためのポイントを解説しています。

2025年の活動紹介
インプリメンテーション研究会

認識合わせ

マネジメントレビュー

DX/AI

■2025年インプリメンテーション研究会の活動　3テーマ

テーマA：認識合わせ

認識の齟齬によるコミュニケーションエラーの事例＆対策に関する提案

各ステークホルダー間の認識違いなどによって発生するISMS関連の無駄稼働の削減＆効率化事例を例示することで認証組織に対する悩み解決の情報提供

テーマB：マネジメントレビュー　・・・　抜粋版でご紹介

マネジメントレビューに関する具体的な事例紹介＆効果的な運用に関する提案

各組織で実施しているマネジメントレビューの実態（議題や付議タイミング）について具体的な運用実態の紹介＆多忙なマネジメント層との効果的なコミュニケーションを模索する

テーマC：DX/AI

「ISMSにおける課題」を解決するためのDX/AI活用に関する提案

「ISMSにおける課題」を解決するためのひとつの模索としてDX/AI活用事例の列挙と深堀りを行うとともに、DX/AIを推進する上での課題を可視化する

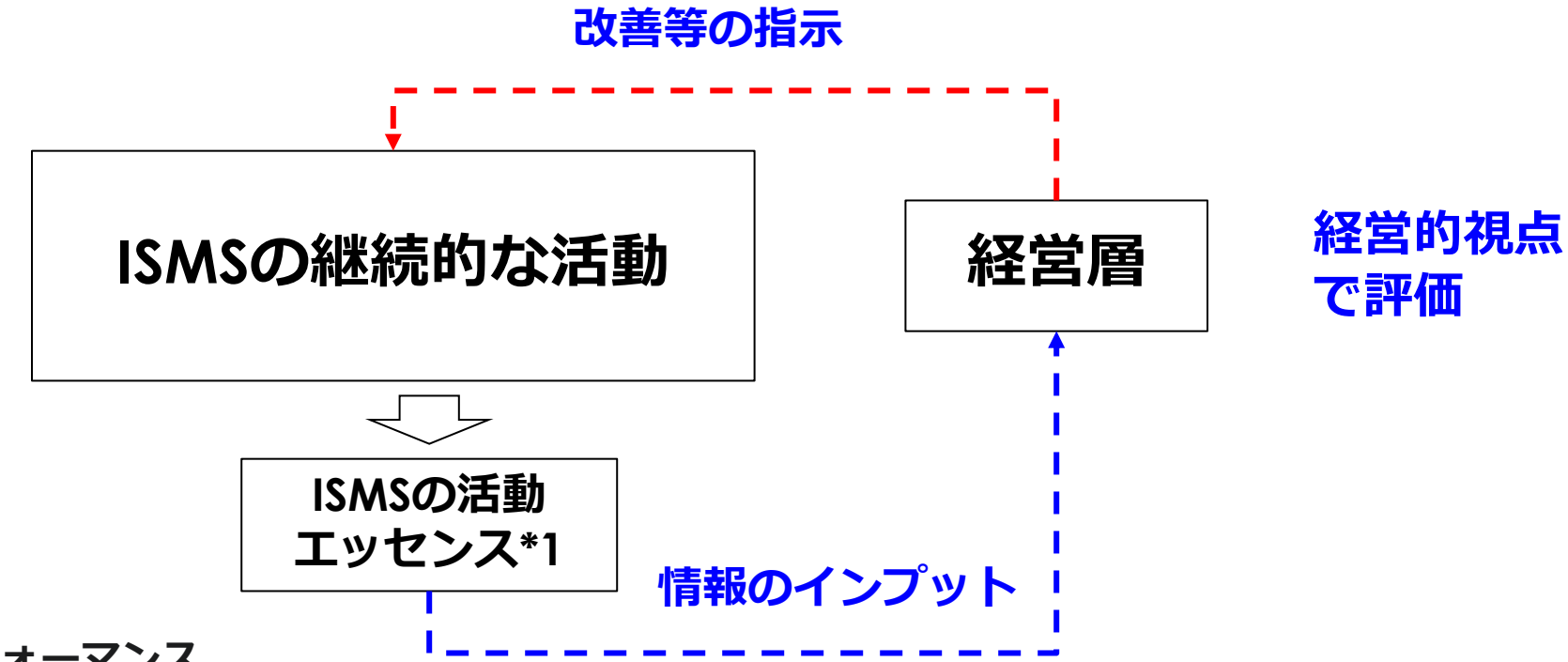
脱・形骸化！ISMSを動かすための「実効的マネジメントレビュー」実践論

情報セキュリティマネジメントセミナー2025の講演資料より

抜粋版

マネジメントレビューの位置付け

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
確認する極めて重要な営み

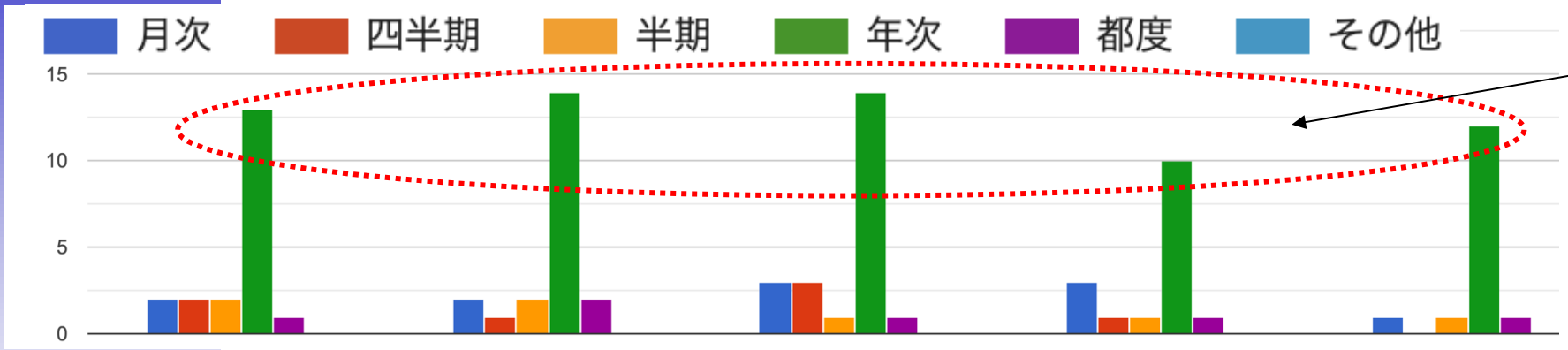


*1：ISMSのパフォーマンス
に関する様々なデータ

年1回のマネジメントレビューの謎？について

参考資料

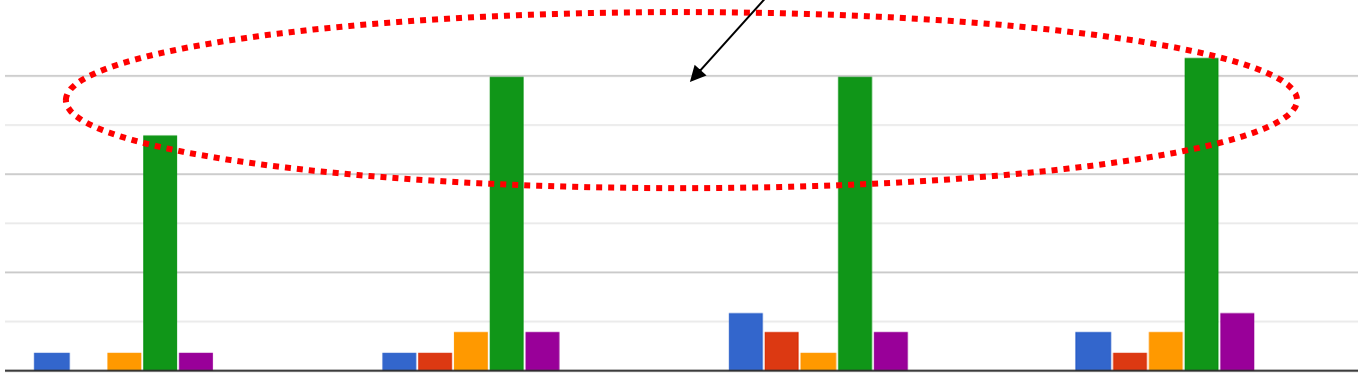
マネジメントレビューの議題（トピック）と付議のタイミングの実態（アンケート結果）



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　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



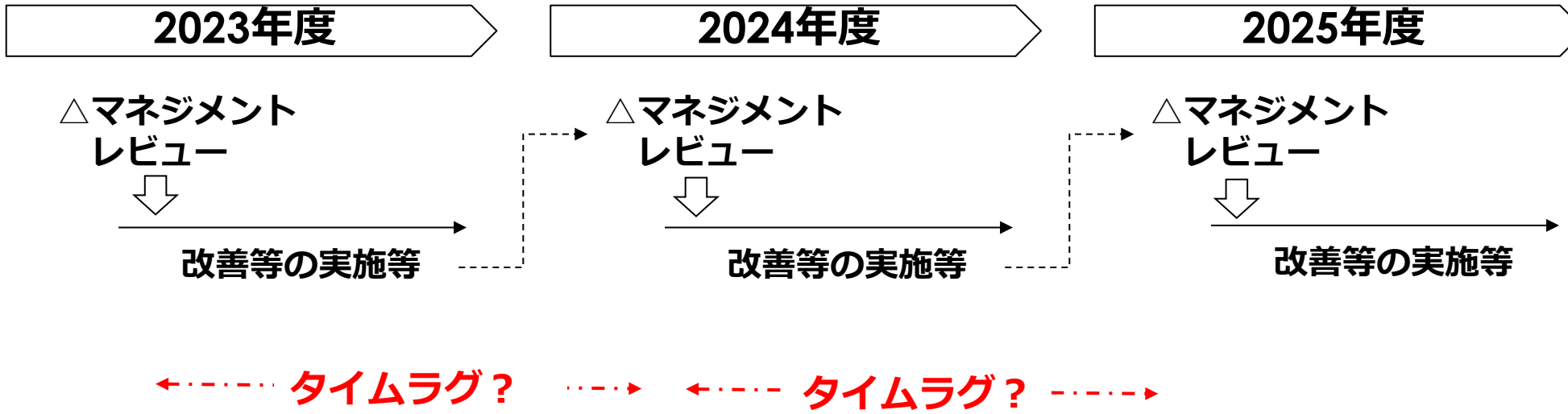
d)情報セキュリティパフォーマンス 4)目的の達成　e)利害関係者のフィードバック　f)リスクアセスメントの結果、対応状況　g)継続的改善の機会

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

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

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

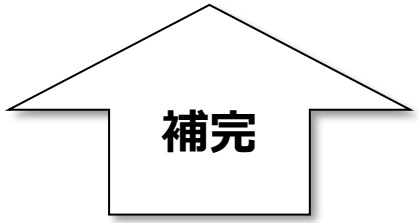
間隔	会議体、付議項目	備　考
日次	日々のモニタリングレポート	日常的なレポートライン
週次	週次のモニタリングレポート	日常的なレポートライン
月次	インシデントレポート	傾向分析含めた組織の健康状態
四半期	セキュリティ委員会	CISO中心としてマネジメントレビューを補完する実務活動
半期	年間計画（予算等リソース審議含む）	マネジメントレビュー相当
年次	トップマネジメントレビュー（総括）	マネジメントレビュー
随時	緊急インシデント対応の相談など突発事項（報連相）	重大インシデントや緊急な経営判断が必要な案件

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）

マネジメントレビュー
の具体事例紹介

抜粋版

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**

抜粋版

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

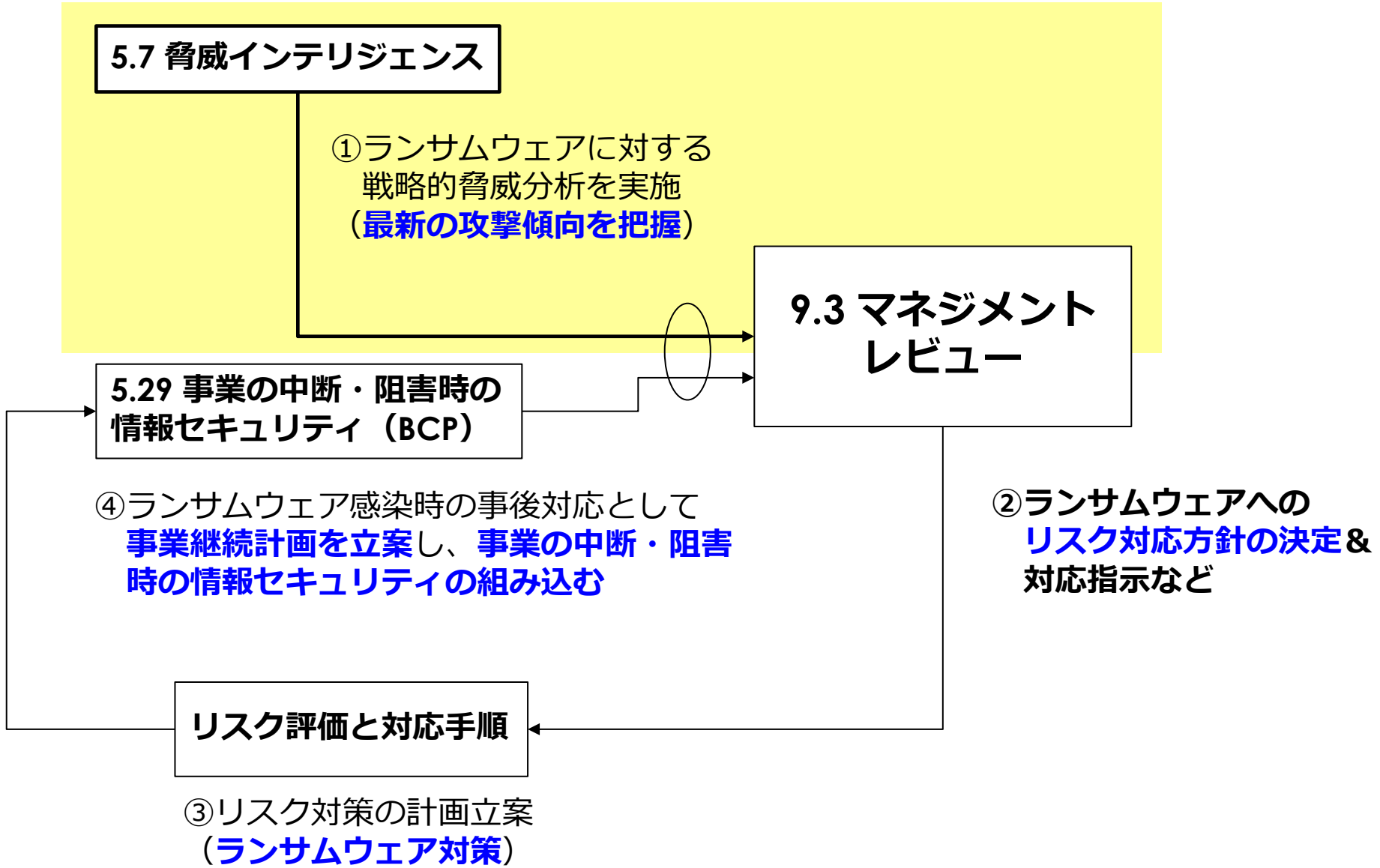
情報セキュリティの**脅威に関する情報を収集及び分析し、脅威インテリジェンスを構築**することが求められているので、箇条5.7の活動結果をインプットとして情報を整理してインプットする

↓

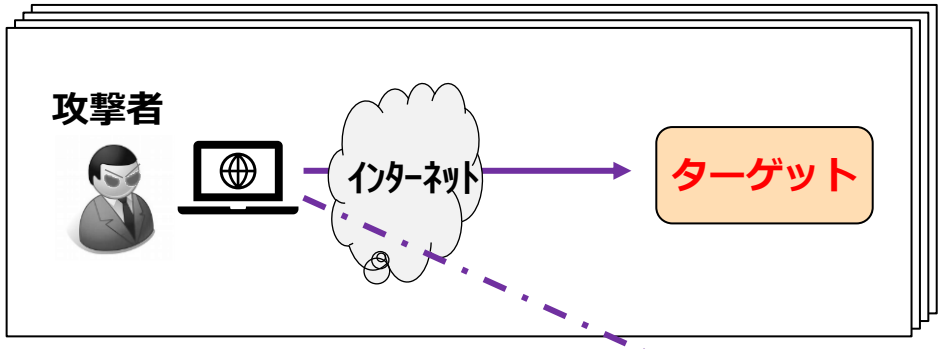
戦略情報として判断に必要な情報

- 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。

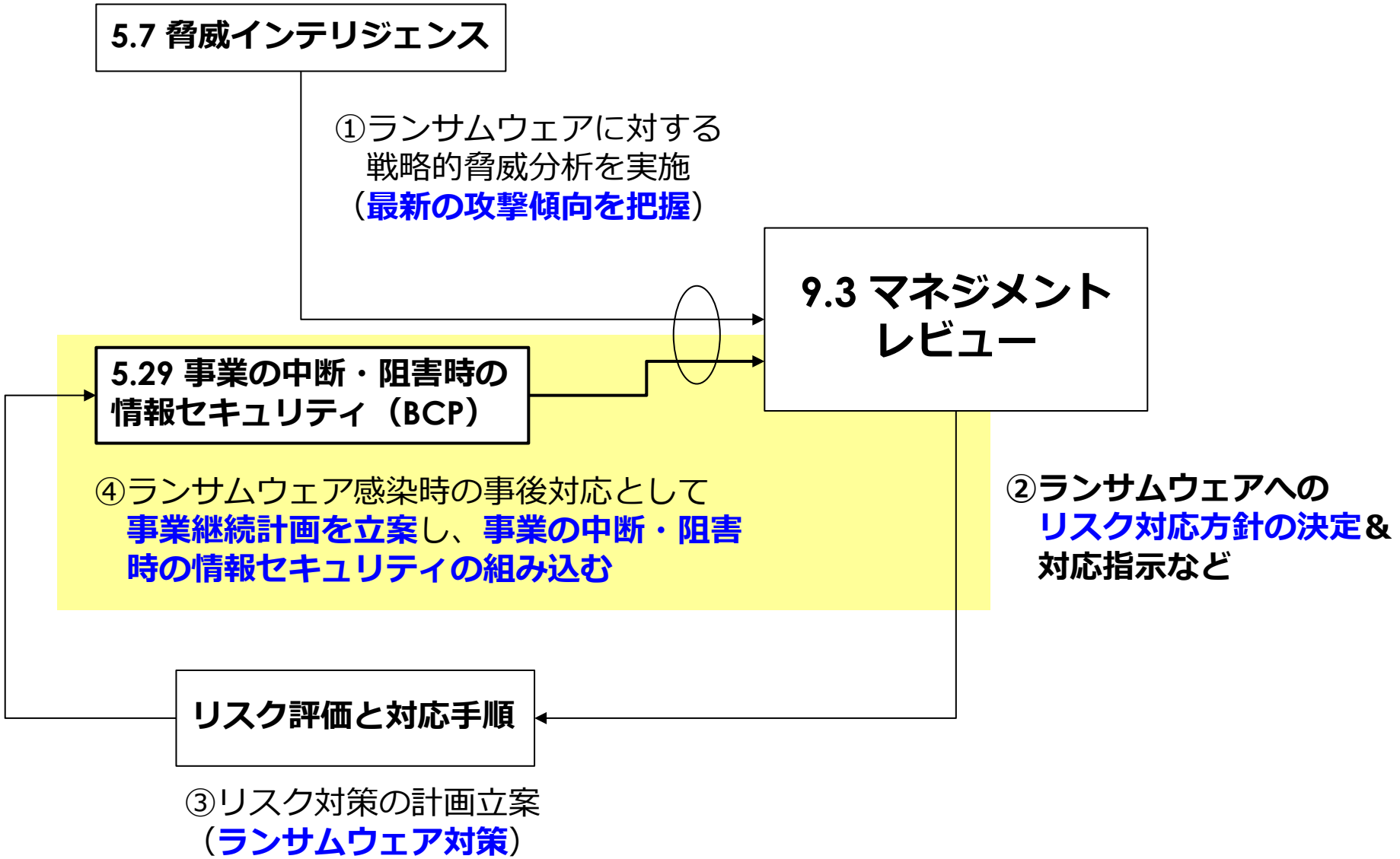
*1：Tactics, Techniques, and Procedures

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

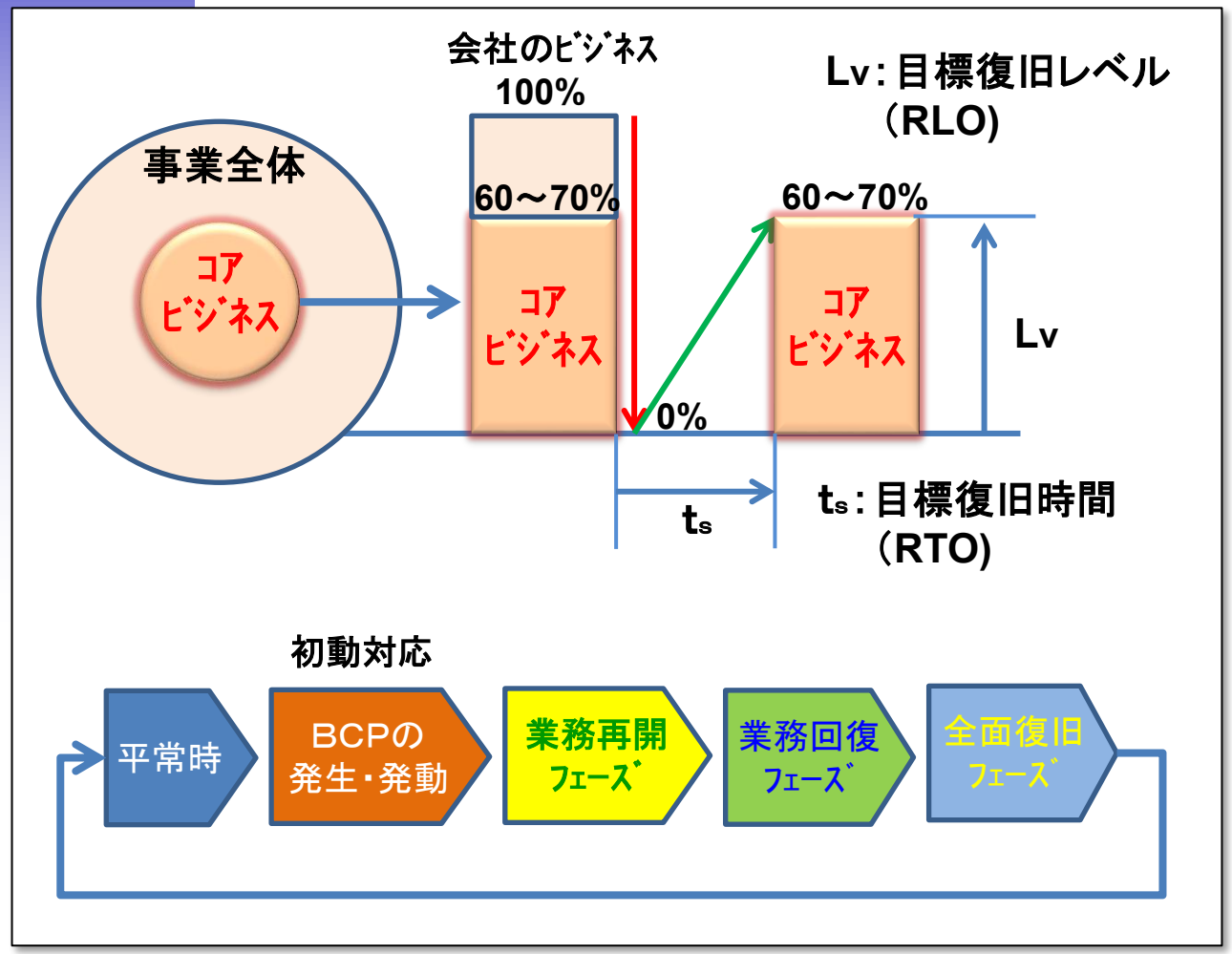
ランサムウェア対策とマネジメントレビュー



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

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

＋

形式的にならないために

・インプット情報の質と量（**良質なインプット情報**）

→情報不足や不正確で適切に判断出来ない、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**）

→決定した改善策や必要な資源の提供が実行されない、遅延を防止
→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**）

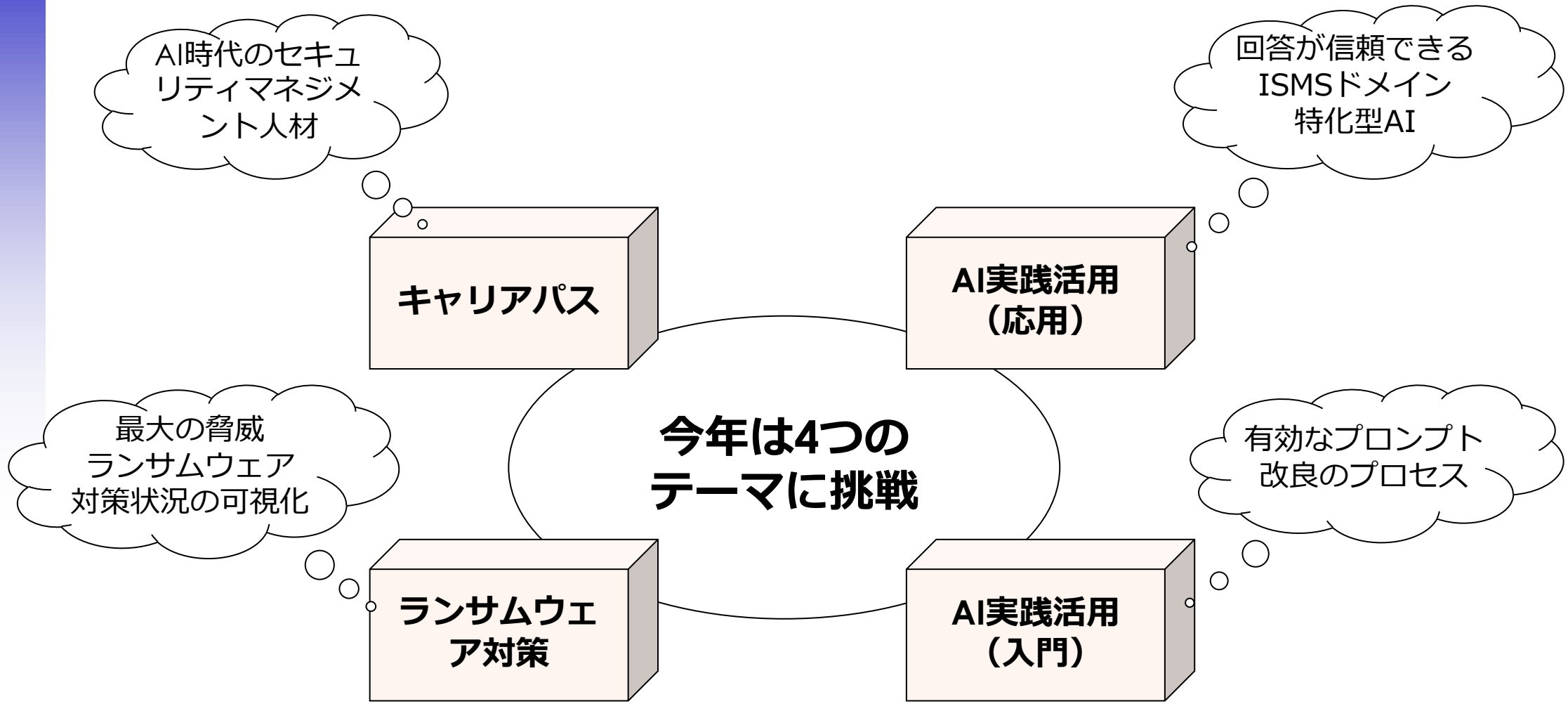
→情報セキュリティをコストではなく投資やビジネス上の優位性として理解

2026年の活動紹介
インプリメンテーション研究会

今年も活発に活動しています

少しだけご紹介

インプリ研の4つのテーマ（進行中）・・・組織をとりまく最新の課題



テーマ（キャリアパス）

AIガバナンス時代を生き抜く
「次世代セキュリティマネジメント人材」の育て方

(現場の泥臭さを「最強のポータブルスキル」に
変えるキャリアロードマップ)

テーマリーダー：尾崎　（株）Speee

AI時代、なぜ「ISMS事務局経験」が最強のキャリア資産になるのか

～現場を知るアーキテクトだけが未来を変えられる～

生成AI普及の影に潜む「スキルの空洞化」

業務効率化の裏で進む思考の丸投げが招く致命的なリスクと、AIの巧妙な嘘（ハルシネーション）を見抜くための問題提起を行います。

「退屈な番人」から「組織のアーキテクト」へ

単なる認証維持のための雑務係（形骸化した運用）にとどまらず、組織の仕組みを根本から書き換えるクリエイティブな本質について切り込みます。

認知の偏りを解き明かす「2つのメタファー」

セキュリティマネジメント職が直面する評価の理不尽さや、世間のイメージとのギャップを、誰もが直感的に納得できる鮮烈な比喩を用いて解説します。

AI時代、なぜ「ISMS事務局経験」が最強のキャリア資産になるのか

～現場を知るアーキテクトだけが未来を変えられる～

全部門を見渡せる特権と重要スキル

組織全体のビジネス構造を鳥瞰できる事務局だからこそ培われる、現場と経営を繋ぐ「翻訳力」や「調整力」の本質に迫ります。

専門家の壁と市場価値を高めるパス

若手や未経験者が陥りがちなバイアスを明かしつつ、今後需要が高まる領域や、将来的に世界のルールを創る側・経営層（CISO）へと至る3大パターンを示します。

AI社会で代替不可能となる「野生の勘」

一見「非効率」とも思える自力での泥臭い格闘 of 経験が、20年後になぜ代替不可能な最強のキャリア資産になり得るのか、その確信をお伝えします。

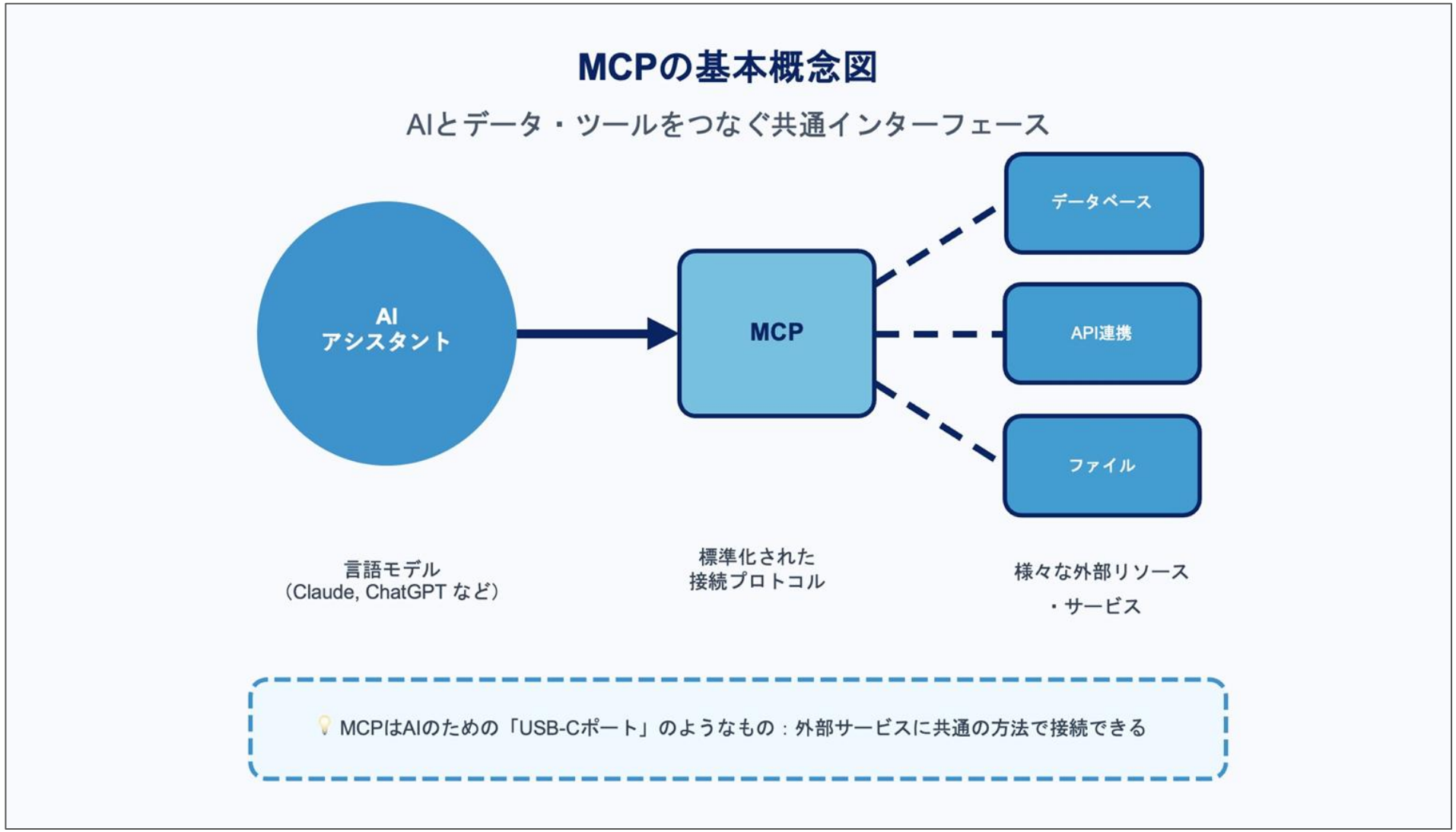
回答が信頼できる
ISMSドメイン特化型AIを作る

狙い：ISMS 担当者の普段の業務に役立つISMSドメイン特化型AI

目指す方向性：ISMSコンサルタントと同等の回答が得られる

テーマリーダー：井崎（SecureNavi株式会社）

MCPサーバのイメージ



参考情報

特権アカウント管理の注意ポイント、要点についてまとめて

素のOpenAI

PURE 素のOpenAI　　ツールなし

以下は、特権アカウント管理の注意ポイント・要点です。

1. 特権アカウントを把握する

まず、どのアカウントが特権を持っているかを正確に把握することが重要です。

2. 最小権限の原則を徹底する

特権は必要な人に、必要な期間だけ、必要な範囲で付与します。

注意点：

- 常時管理者権限を付与しない
- 業務に不要な権限を与えない
- 一般業務用アカウントと管理用アカウントを分離する
- 退職者・異動者の権限を速やかに削除する

理想的には、必要な時だけ一時的に権限を付与する「Just-In-Time」方式が望ましいです。

3. 共有アカウントの利用を最小化する

`Administrator` や `root` などの共有管理者アカウントは、誰が操作したか追跡しにくくなります。

対策：

- 個人ごとの管理者アカウントを発行する
- 共有アカウントの利用は原則禁止または限定する
- やむを得ず使う場合は利用申請・承認・記録を残す
- 操作ログやセッション録画を取得する

4. 多要素認証を導入する

特権アカウントは攻撃者の主要な標的です。IDとパスワードだけでは不十分です。

対策：

- MFA、多要素認証を必須化する
- 管理コンソール、VPN、クラウド管理画面に適用する

MCP接続OpenAI

MCP MCP接続OpenAI　　公開参照資料ツール接続

以下は、ISMS運用における**特権アカウント管理の注意ポイント・要点**です。
特権アカウントは、サーバ、ネットワーク機器、クラウド、DB、業務システム、ID基盤などに対して強い操作権限を持つため、通常アカウントよりも厳格に管理する必要があります。

2. 管理の基本方針

特権アカウント管理の基本は、次の考え方です。

観点	要点
最小権限	必要な人に、必要な期間、必要な範囲だけ付与する
個人識別	共用IDの使用を避け、誰が操作したか追跡できるようにする
承認制	付与・変更・削除には責任者承認を必要とする
記録	ログイン、操作、権限変更、設定変更を記録する
定期確認	棚卸しにより不要・過剰な権限を削除する
強い認証	多要素認証、強固なパスワード、鍵管理を適用する
緊急時管理	緊急用IDの利用条件、承認、事後確認を明確にする

ISMSでは、リスクアセスメントやリスク対応で決めた管理策を、実際の運用プロセスに組み込んで管理することが重要です。JIPDECのISMSユーザーズガイドでも、運用の計画策定及び管理において、リスクアセスメントやリスク対応の活動を運用プロセスに組み込む観点が示されています[1]。

3. 注意ポイント

3.1 特権IDの一覧化

まず、どこに特権アカウントが存在するかを把握します。

確認対象の例：

- OS管理者ID
- AD、Entra ID、LDAPなどのID基盤

MCP接続OpenAI

ISMSの運用における具体的なプロンプトを集めた実践事例集的なまとめ

プロンプト改良のプロセスの有効な手法と
実践事例集の提供

テーマリーダー：川澄　フューチャーセキュアウェイブ株式会社

テーマ：プロンプト改良のプロセス

- 背景：
  - これまでの研究会ではAIや脅威インテリジェンス等の概念整理を行ってきたが、**具体的な実践事例**の研究は不足していた
- 研究の着眼点：
  - 技術スキルが乏しいISMS事務局でも、AIを活用することでISMS活動の実務・品質向上ができることを示す
- 研究のアプローチ：
  - 「どのようなプロンプトが有効か」を体系的に検証し、**プロンプト改良のプロセスごと成果物**として提示する

成果物候補

- 成果物として研究素材となるプロンプト入力例と出力結果とプロンプト改良のプロセス（品質向上のTips）を提供予定

JSON

```
{
  "1_最新の情報セキュリティ脅威の特定": {
    "対象となる主要な脅威の名称": [
      "1. クラウドサービス(Box/SharePoint/MS-365)を標的としたアカウント乗っ取り",
      "2. 外部パートナーを経由したサプライチェーン攻撃",
      "3. 生成 AI(Copilot 等)悪用による高度なフィッシング詐欺およびデータ侵害"
    ],
    "それぞれの脅威について具体的な攻撃手口と特徴": [
      "1. アカウント乗っ取り:従来の ID・パスワード窃取だけでなく、二要素認証(MFA)を突破する『AiTM(Adversary-in-the-Middle:中間者攻撃)※1』フィッシングが激増。セッショントークン(ログイン状態を維持する情報)を盗み出し、クラウド(Box や SharePoint)に直接サインインして、特許申請前のデザインデータや個人情報を一括ダウンロードする手口が主流です。",
      "2. サリプチェーン攻撃:セキュリティが強固な本部ではなく、防衛の手薄な個人事業主(外部パートナー)の端末を『踏み台※2』にします。パートナーになりすまして業務連絡メール(Outlook)を送り、Box の共有リンクに見せかけたマルウェア(悪意あるプログラム)を実行させたり、正規の共有フォルダ内のデータを改ざん・窃取したりします。",
      "3. 生成 AI の悪用:攻撃者が生成 AI(LLM)を用いて、極めて自然で組織の文脈に合致した『ビジネスメール詐欺(BEC)※3』の手紙文を作成します。また、社内ユーザーが適切な権限設定(ACL)を怠ったまま『Copilot』を利用した結果、本来閲覧権限のない従業員や外部アカウントに、意匠・特許の重要情報が AI の回答経由で漏洩する『内部データプロンプトインジェクション/権限逸脱※4』リスクも顕在化しています。"
    ]
  },
  "2_組織の現状と想定されるリスク": {
    "想定される最大の被害シナリオ": "最悪のシナリオは『外部パートナー経由で Box のアカウントが乗っ取られ、意匠登録・特許申請前の新製品アイデアが競合他社や海外へ流出、同時に直販サイトのバックエンドである販売管理(SharePoint)から顧客の個人情報が漏洩する』事態です。アイデア流出により先行優位性と数億円規模の見込み利益が喪失し、個人情報漏洩による損害賠償とブランド失墜で Amazon・直販サイト双方の売上が激減。さらに決済代行会社からの信頼を失い、クレジットカード決済の利用停止処分を
```


出力結果

＋

プロンプト改良のプロセス

ChatGPT


```
{
"1_最新の情報セキュリティ脅威の特定": {
"対象となる主要な脅威の名称": [
"ランサムウェア攻撃(データ窃取＋暗号化の二重脅迫型)",
"ID・認証情報を狙う攻撃(Microsoft 365、Box、SharePoint 等のクラウドアカウント侵害)",
"サプライチェーン攻撃(委託先、パートナー、ソフトウェア更新経路の悪用)",
"生成 AI・Copilot 利用に伴う情報漏えいリスク",
"ビジネスメール詐欺(BEC)および AI 利用型フィッシング",
"知的財産(アイデア・設計図・意匠・特許情報)を狙う標的型攻撃",
"クラウドサービス設定不備・過剰権限による情報漏えい",
"内部不正および退職者・パートナーによる情報持ち出し"
],
"それぞれの脅威について具体的な攻撃手口と特徴": [
{
"脅威": "ランサムウェア攻撃",
"攻撃手口": [
"フィッシングメールから認証情報を窃取",
"クラウドアカウントを乗っ取り内部へ侵入",
"データを窃取後に暗号化し、身代金を要求",
"バックアップや共有フォルダも同時に破壊"
],
"特徴": "2025～2026 年は『まずデータを盗み、その後暗号化する』二重脅迫型が主流。AI 活用により攻撃速度が大幅に向上している。"
},
{
"脅威": "ID・認証情報を狙う攻撃",
"攻撃手口": [
"Microsoft 365 や Copilot を装った偽ログイン画面",
"音声電話によるなりすまし(Vishing)",
"セッションハイジャックによる認証情報の窃取",
"多要素認証を回避する中間者攻撃(AiTM)"
],
"特徴": "近年は『侵入する』より『正規 ID でログインする』攻撃が増加している。"
},
{
"脅威": "サプライチェーン攻撃",
"攻撃手口": [
```

テーマ（ランサムウェア対策）

規格要求事項から見た
ランサムウェア対策状況の可視化

- 基本のキ（予防保全、事後対策）
- ルールの実行状況の可視化（モニタリング）
- 経営者が説明責任を果たせる

テーマリーダー：魚脇　NTTドコモビジネス（株）

本テーマの背景＆目指す姿

➢ テーマの背景＆狙い

脅威のトップに位置付けられるランサムウェア
規格要求事項から見たランサムウェア対策状況の可視化
対策状況（ガバナンスの状態）をGreen/Yellow/Redで可視化

➢ 基本的な前提

ランサムウェアは完全には防げない＆**侵入要因の多くは基本動作の不備**
→　**予防保全と事後対策の両輪**で備える

➢ 対策の3つの柱

① 基本動作の徹底（脆弱性管理・認証・特権管理・監視など）
② 最後の砦：バックアップ＆リカバリ（イミュータブルBU・隔離保管・復旧訓練）
③ エビデンスに基づく可視化＆モニタリング（証跡で確認・ダッシュボード化）

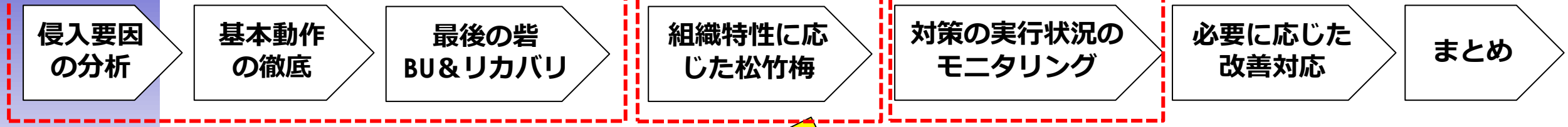
➢ 目指す姿

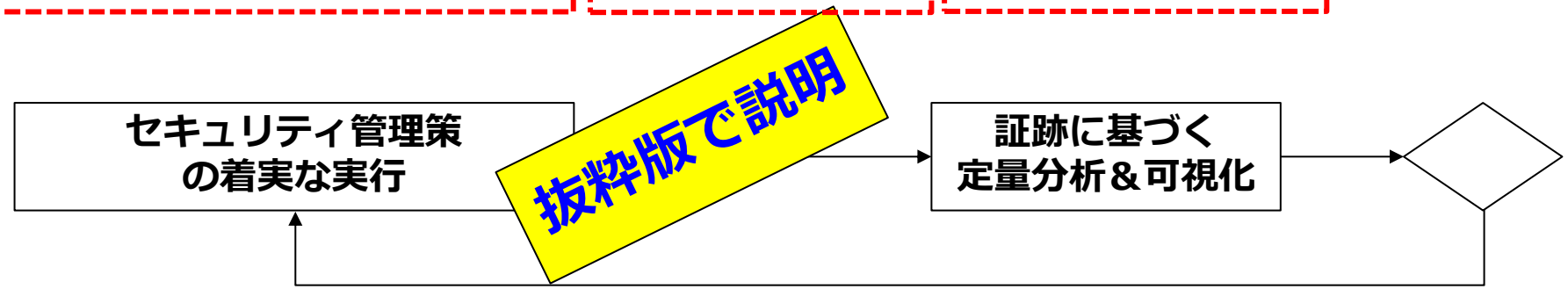
基本動作の徹底＆モニタリングの実施
組織の状況に応じた**「松竹梅」の対策レベル設定**
経営層への説明責任の確保

テーマの全体構成（案）

★基本動作が守られていない！

その1　その2　その3　レベル設定　可視化





Yellow/Redの場合に改善の実施

成果物イメージ（案）

やるべき項目＆ポイントの明確化、事例の紹介など	対応レベルの考え方（案）	Green/Yellow/Redの判断基準 弱点の可視化＆マネジメント層との共有など

ランサムウェアのインシデント事例分析（侵入要因）

侵入要因（公表ベース）・・・抜粋

事例	侵入要因
A社	従業員アカウントに対する**フィッシング攻撃による認証情報の窃取**
B社	**取引先側のIT環境が侵入口となったサプライチェーン攻撃**、**リモート接続環境の脆弱性**が指摘
C社	委託業者が使用していた**VPN機器の脆弱性**を悪用、医療機関自身ではなく**「委託先経由」の侵入**
D社	**グループ拠点のネットワーク機器を経由**、**管理者パスワードの脆弱性悪用権限奪取後**、**業務時間外に内部探索**を実施

- **VPN・ルータ等ネットワーク機器の脆弱性放置**
- **フィッシングによる認証情報窃取**
- **委託先・取引先を含むサプライチェーンの管理不足**
- **管理者権限・パスワード管理の不備**
- **休日・夜間を狙った活動による**

普段から当たり前に管理プロセスとして実行しているはず？

基本動作の徹底（脆弱性管理）

分類	基本動作（保守・運用の日常業務として）
脆弱性管理	・利用している製品の脆弱性情報の入手し、緊急度に応じた迅速なアップデートの実施 ・緊急度の低いものは定期的（月次、四半期）でメンテナンスを実施する ・EOS/EOL製品の利用禁止や移行計画の策定＆着実な実施（VPN製品の廃止など）

Q.1：構成管理として全ての利用製品一覧と脆弱性情報を把握していますか？
（抜け漏れは？脆弱性情報はタイムリーに入手出来ていますか？）

Q.2：入手した脆弱性情報の緊急度に応じてシステムアップデートを実施していますか？
（時間単位での対応や自システムへの影響度判断など）

Q.3：緊急度の低いものを放置していませんか？
（緊急度が低くても影響がないわけではありません）

Q.4：サポート切れ（EOS/EOL製品）を使い続けていませんか？
（鍵の壊れた金庫を放置しているような状態になっていませんか？）

その3

リカバリ手順の比較表（一般/ランサムウェア）

比較項目	一般的なリカバリ手順 (機器故障・災害・誤消去など)	ランサムウェアにおけるリカバリ手順 (サイバー攻撃対応)
主目的	業務の早期再開（スピード重視）	**安全性が確認された状態での**業務再開 （二次被害防止重視）
環境の隔離	不要（ネットワークは接続したまま）	**必須**（感染拡大を防ぐため、完全なネットワーク隔離環境で行う）
バックアップの安全性確認	不要（最新のデータからそのまま戻す）	**必須**（バックアップデータ自体が汚染・暗号化されていないかスキャンする） **1ヶ月以上の潜伏型へ対応するにはバックアップデータとして1ヶ月以上の保管期間と世代管理が必要**
OS・システム一新	状況に応じて（基本はデータのみ復旧）	**原則必須**（OSの初期化、またはクリーンなイメージからの再構築）
リカバリ「後」のチェック作業	データの整合性チェック、動作確認	**厳重な感染有無チェック、パッチ適用、脆弱性の修正、監視（EDR等）の強化**
根本原因の対策	故障部品の交換、手順の見直し	侵入経路の特定と遮断（同じ方法で再感染するのを防ぐ）

その3

ランサムウェア復旧時 特有の重要プロセス

一般的なリカバリ　　：「元通りに戻す作業」

ランサムウェアのリカバリ：「デジタル犯罪現場の調査・消毒を行いながら、安全なサイバー空間を再構築する作業」

1. 隔離環境（サンドボックス）での復旧

クリーン環境（ネットワークから隔離されたセーフハウス的な環境）を用意し、そこで一度システムを復旧させる（いきなり本番ネットワークに戻してはいけない）

2. リカバリ直後の「潜伏調査（クレンジング）」

データを書き戻した直後、およびシステム起動後に、以下のような徹底的なチェックを実施

・最新の定義ファイルを使用したマルウェアスキャン
・不審なレジストリ、スケジュールタスク、自動起動設定の有無確認
・バックドア（攻撃者が残した裏口）が仕込まれていないかの検証

3. 脆弱性の修正（再感染防止）

ランサムウェアが侵入した「原因（OSの脆弱性、VPNの欠陥、弱いパスワードなど）」を修正してからでないと、復旧した瞬間に再度暗号化されるリスク（再感染）がある

4. 復旧後の「継続監視」

本番ネットワークに戻した後も、しばらくの間はEDRなどの監視ツールを「高感度」に設定し、不審な挙動（再発）がないかを注視　する必要がある

レベル設定

ランサムウェア対策の松竹梅の考え方（案）

＜　整理の方針案　＞

松

・AI-SOCの導入
・24/365の相関分析と監視

＋β　AIの攻撃にAIで対応
対応スピード、網羅性

竹

・ランサムウェア対策ソリューションの導入
・CSIRT体制の構築＆運用

＋α　防御、検知の充実
対応体制の強化＆準備

梅

・基本的なセキュリティ対策の実装
（基本動作の徹底）
・バックアップ/リカバリ対策の実装
（ランサムウェアに対応した要件）

最低限のベースライン

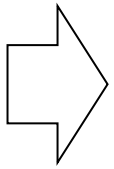
基本動作の徹底
（防御、BU＆リカバリ）
実施状況のモニタリング

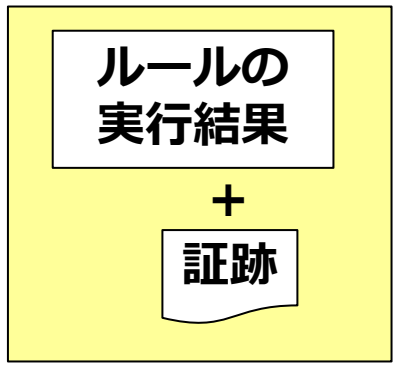
管理策の確実な実行とモニタリング

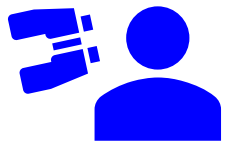
現状の課題と本テーマの目指す姿

項目	現状の課題（口頭確認）	本テーマが目指す姿（証跡に基づく確認）
評価軸	担当者の主観や「導入済み」という事実のみ	**規格要求事項＋エビデンスに基づいた客観的スコアリング**
管理範囲	侵入防御（入り口）に偏重	**予防**（基本的な管理策）**＋事後**（バックアップ）**の包括的評価**
可視化	インシデントが起きるまで「不明」	**シグナル（Green/Yellow/Red）による ガバナンス状態の可視化**＆常時モニタリング

やっていますという口頭報告（実態との乖離）







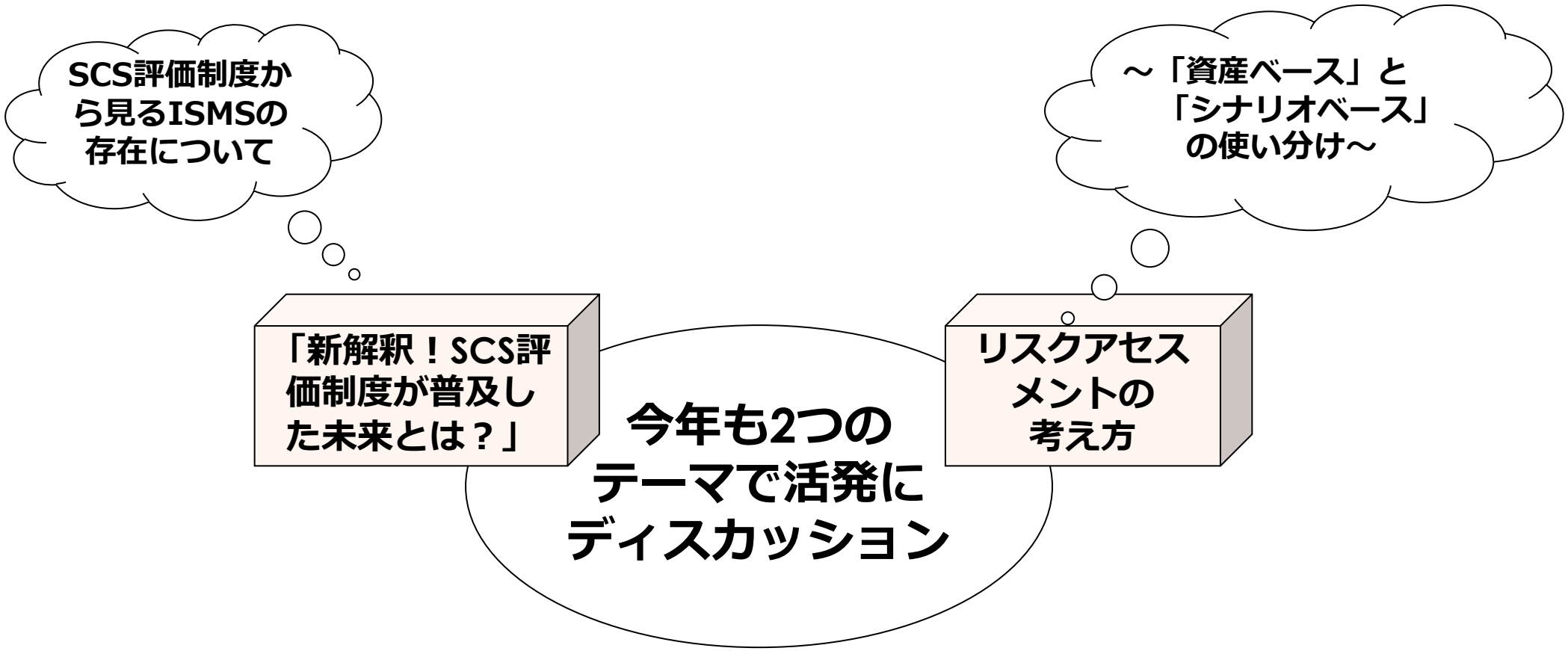
ルールの実行した結果として発生する証跡を添付することでガバナンス状態を可視化

ライトニングトーク（Lightning talks）形式*1による勉強会の開催について

・5～10分の短い発表（2テーマを1時間で）
・問題定期＆ディスカッション
・異なる意見やディスカッションから得られる新たな気づき
・気軽に参加出来る

*1：ライトニングトーク（Lightning talks）はLTと略される短いプレゼンテーション
（稲妻（Lightning）のようにスピード感のあるプレゼンテーションという意味合い）

LT（ライトニングトーク）形式勉強会の2つのテーマ・・・進行中



2026年LT形式勉強会テーマ（案）

テーマ1

「新解釈！SCS評価制度が普及した未来とは？」

情報セキュリティマネジメントシステム（ISMS）と
SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）
の比較など

テーマ担当：山口　富士ソフト（株）

テーマ2

どっちで考えるリスクアセスメント
～「資産ベース」と「シナリオベース」の使い分け～

網羅的な「静」の分析（資産ベース）と具体的な「動」の分析
（シナリオベース）の２つの手法の比較＆ディスカッション

テーマ担当：北村　一般社団法人 情報処理安全確保支援士会

テーマ1（「新解釈！SCS評価制度が普及した未来とは？」）

絶対王者ISMSに挑む
期待の新星！SCS評価制度

★3

★4

何故ISMS取得企業でもSCS評価制度に苦戦するのか！？
SCS評価制度だけでは解決できない“ある問題”とは･･･。

あなたの会社は本当に対応出来ていますか？

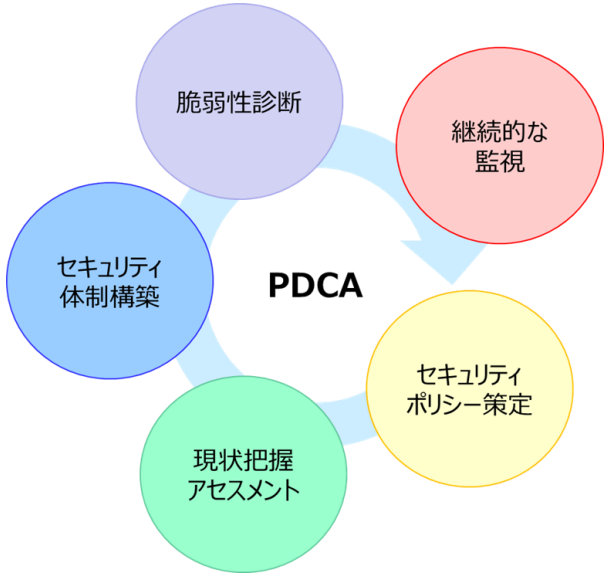
ISO27001

ISO27002

SCS評価制度で再注目されるISMSの価値とは？

SCS評価制度は、ISMSをベースに外部拡張版、そして実務強化したものと言えます。
但し、それだけでは十分だと言い切れません。

項目	ISMS	SCS評価制度
視点	自社中心	サプライチェーン全体
特徴	仕組み・文書重視	実務・運用重視
委託先	管理対象の一部	主役レベルで重要



SCS評価制度で、チェックシート埋めるだけや、
管理策を対応するだけでは、
企業としての信頼を十分に得る事が出来ない。

継続的な見直しが必要

- **社会全体のセキュリティレベル向上**
- **セキュリティレベルの向上に繋げるには相互補完が必要**
- **各企業や人々のセキュリティ意識の向上なので、セキュリティ人材不足が起こらない世界を想像・・・**

テーマ2（どっちで考える？リスクアセスメント）

～「資産ベース」と「シナリオベース」の使い分け～

詳細リスク分析の２つの手法、資産ベースのリスク分析とシナリオベースのリスク分析について、国内にあるいくつかの利用ガイドからそれぞれの特徴と使い方をご提案＆ディスカッションしましょう！

- **「地図を作る」か「シミュレーションするか」**

比較項目	資産ベース（ガイドライン）	シナリオベース（キット）
アプローチ	ボトムアップ（積み上げ）	トップダウン（目的志向）
重視すること	**網羅性**（漏れをなくす）	**具体性**（対策を絞る）
成果物	リスク評価値付きの資産台帳	攻撃・事故の推移シナリオ
適した場面	ISMS構築、全体把握	事故訓練、経営層への説明

■ LT（ライトニングトーク）形式による勉強会

（27000シリーズの最新動向とベストプラクティスの提案）

2026年9月15日（火）
13:00～14:00　リモート形式

JNSA

開催予告

◆ LT（ライトニングトーク）形式による勉強会◆
ISMSの身近なテーマを題材としたディスカッション　～気軽に参加してみませんか？～

日本ISMSユーザーグループでは誰でも参加出来る気軽な勉強会を開催します。
今回扱うテーマは下記の2つのテーマを取り上げます。

テーマ1は情報セキュリティマネジメントシステム（ISMS）とSCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）の比較などについて紐解きます。
テーマ2は網羅的な「静」の分析（資産ベース）と具体的な「動」の分析（シナリオベース）の２つの手法の比較を交えて解説します。
ひとつの考え方を情報発信し、テーマ毎にディスカッション出来ればと考えています。
皆さまとのディスカッションを楽しみしていますので、気軽に参加頂ければ幸いです。

テーマ1：「新解釈！SCS評価制度が普及した未来とは？（仮）」

テーマ2：「どっちで考えるリスクアセスメント（仮）」
～「資産ベース」と「シナリオベース」の使い分け～

■情報セキュリティマネジメントセミナー2026

（27000シリーズの最新動向とベストプラクティスの提案）

開催予告

JNSA

2026年12月4日（金）午後　・・・　詳細は別途、案内予定

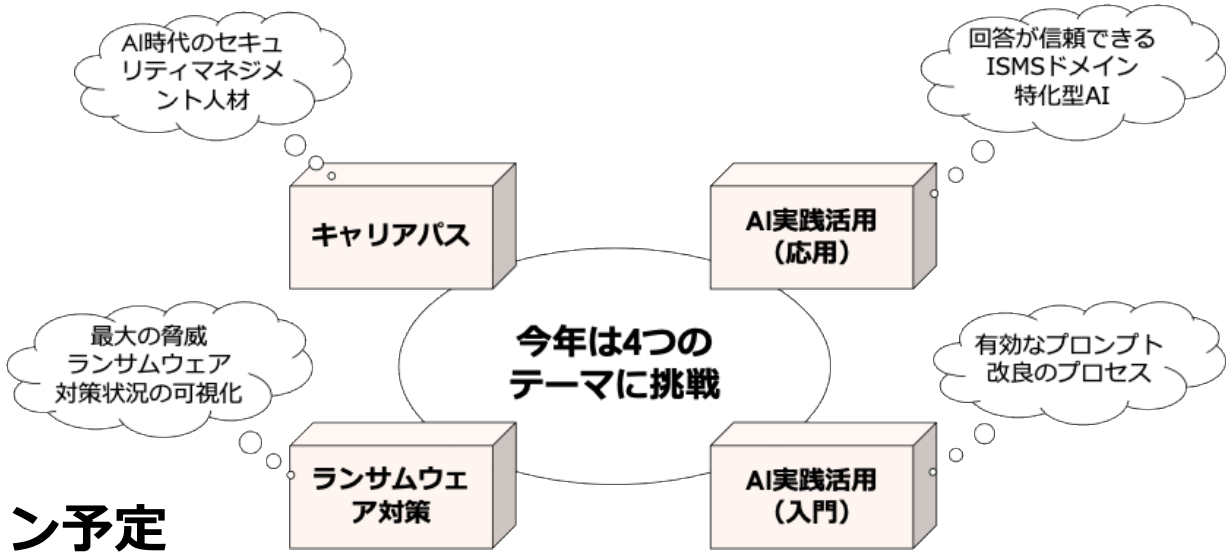
【標準化動向】

ISO27001、ISO27002などの27000シリーズの標準化の最新動向など

【研究会成果報告】

インプリメンテーション研究会の活動成果

テーマ1：「キャリアパス」
テーマ2：「ランサムウェア対策」
テーマ3：「AI実践活用（応用）」
テーマ4：「AI実践活用（入門）」



【パネルディスカッション】

最新のトピックについてディスカッション予定

60

■インプリメンテーション研究会へのお誘い

毎年、**組織を取り巻く環境の変化に対応したテーマに挑戦**して ISMSの構築・運用に
おけるベストプラクティクスを検討しています。
ご興味のある方は一緒に検討に参加頂ければ幸いです。
冷やかしも大歓迎ですので、気軽にJNSA事務局へご連絡ください。

テーマ1： キャリパス
テーマ2： ランサムウェア対策
テーマ3： AI実践活用（応用）
テーマ4： AI実践活用（入門）

開催形式：ハイブリッド（リアル会場＋Web会議）

毎月最終木曜日18:00～21:00開催

＋