情報セキュリティマネジメント・セミナー2025
パネルディスカッション

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～

パネリストのご紹介

パネリスト			パネリストの立場
ISMS-AC	保木野 昌稔 氏	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）	ISMSのその信頼性の向上と維持に向けて活動している認定機関としてのアドバイス
SC27/WG1	土屋 直子 氏	ISO/IEC JTC1/SC27 WG1小委員会 （NTTテクノクロス株式会社）	標準化の観点でのアドバイス
	羽田 卓郎 氏	日本ISMSユーザグループインプリメンテーション研究会｜ISO/IEC JTC1/SC27 WG1小委員会リエゾン（羽田情報セキュリティ研究所）	
ISMS-UG	北村 俊樹 氏	日本ISMSユーザグループ インプリメンテーション研究会（LINEヤフー株式会社）	規格を具体的に実装する上でのアドバイス
	井崎 友博 氏	標準化部会 日本ISMSユーザグループ　インプリメンテーション研究会 ISO/IEC SC 27/WG 1小委員会　井崎　友博 （SecureNavi株式会社 代表取締役CEO）	

モデレータ：魚脇 雅晴
（標準化部会 日本ISMSユーザグループ WGリーダー
（NTTドコモビジネス株式会社）

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～

ISMS運用を長く続けると、認証が目的化する、環境の変化を見て見ないふりをするなどの「形骸化」という根深い課題に直面することがあります。
本セッションでは、まず現場と経営の認識のズレを埋め、形骸化を防ぐための実践的な「処方箋」について議論します。

認定機関の観点

標準化の視点

Japan Information Security
Management Systems User Group

パネルディスカッション　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～

・土屋 直子 ：ISO/IEC JTC1/SC27 WG1小委員会（NTTテクノクロス株式会社）

・羽田　卓郎：日本ISMSユーザグループインプリメンテーション研究会｜ISO/IEC JTC1/SC27 WG1小委員会リエゾン（羽田情報セキュリティ研究所）

2025年12月5日

なぜISMSの運用が形骸化するのか？　仮説

【標準化チームの仮説】

　ISO/IEC 27001 に基づく ISMS は、本来「形骸化しない仕組み」として設計されている。

　それでも形骸化するのは、構築・運用主体が、ISMS規格（ISO/IEC 27001）のコンセプトや要求事項を正しく解釈し運用していないためではないか。

⇒ 経営のリーダーシップがあり、事務局と内部監査体制が機能している組織では、形骸化はほとんど見られない。

なぜISMSの運用が形骸化するのか？　その1

1. **導入目的が「認証取得」が中心で、経営課題と関連付けされていない**(4.1 、5.2 a))
   - ・トップマネジメントが「取引先要求」「名刺に載る」程度の認識で、課題解決のリーダーシップがない
   - ・その結果、実務に役立たない規程を維持するだけの仕組みとなり、組織課題の解決につながらない
   - ・PDCA が回らず、マネジメントシステムが「作業」と化し、維持・改善の動機が失われる
2. **文書が“運用実態から乖離した理想形”として作成される**(7.5.1 b))
   - ・ 現場運用と手順書が一致せず、審査指摘回避のために要求事項を拡大解釈している
   - ・ チェックリストや記録様式が増え、審査用書類となって実務では参照されない

なぜISMSの運用が形骸化するのか？その2

3. 責任分担が不鮮明で“誰の仕事か”が曖昧（5.3 、7 、A.5.2 ）

・ISMS が「推進事務局の仕事」になり、他部署は当事者意識を持たず、組織全体の活動になっていない

・リスクアセスメント、内部監査、是正処置などが担当者の「個人技」となり、ビジネス活動として人材・時間が割かれていない

4. 内部監査が本来の「改善の機能」を果たしていない（5.1 、7.2 、9.2 ）

・監査員の力量不足により、形式的な「適合性チェック」に終始する（リーダーシップ不足と力量管理の不備）

・「改善の機会」より記録の有無ばかりを確認するような、内部監査プログラムの不備や監査で有効性確認を行うことについての力量不足がある

なぜISMSの運用が形骸化するのか？　その他

5. リスクベースアプローチが十分に機能していない⇒リスク評価とレビューが形式化し、実際の脅威や事業環境の変化を反映できていない(4.1, 6.1.2, 8.2, 9.3.2, A.5.7)
6. KPI／パフォーマンス指標が業務成果とつながっていない⇒ISMS の指標が「件数管理」に留まり、事業価値や成果への貢献が見えない(規格要求事項⇒ 5.1 、9)
7. トップマネジメントのレビューが事務作業化する⇒形式的な年次報告の場となり、意思決定や資源配分の議論が深まらない(5.1 、9.3)
8. 人材流動(担当者入替)で属人化し、仕組みが維持できない⇒担当者交代のたびにノウハウが失われ、仕組みより「人」に依存した運用になる(5.3 、10.1 、A.5.2 、A.8.6)
9. ISMS運用をアウトソース先に依存しており、形骸化する⇒自社の責任と役割が不明確となり、現場の実態と運用ルールが乖離する （ 5.3, 8.1, A.5.2 ）

ISMSへの実装の観点

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～

ISMSの世界でもAI活用という新たな変革の波も訪れています。
本セッションでは、遠く無い未来のテーマに視点を向け、AIは担当者を救うのか、どのように活用するのかについて議論をし、テクノロジーがもたらす効率化の先で人間が担うべき役割とは何かを徹底討論します。

認定機関の観点

標準化の視点

Japan Information Security
Management Systems User Group

パネルディスカッション　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～

- 土屋 直子 ：ISO/IEC JTC1/SC27 WG1小委員会（NTTテクノクロス株式会社）
- 羽田　卓郎：日本ISMSユーザグループインプリメンテーション研究会｜ISO/IEC JTC1/SC27 WG1小委員会リエゾン（羽田情報セキュリティ研究所）

2025年12月5日

ISMS事務局のAI利用で目指したいこととは？

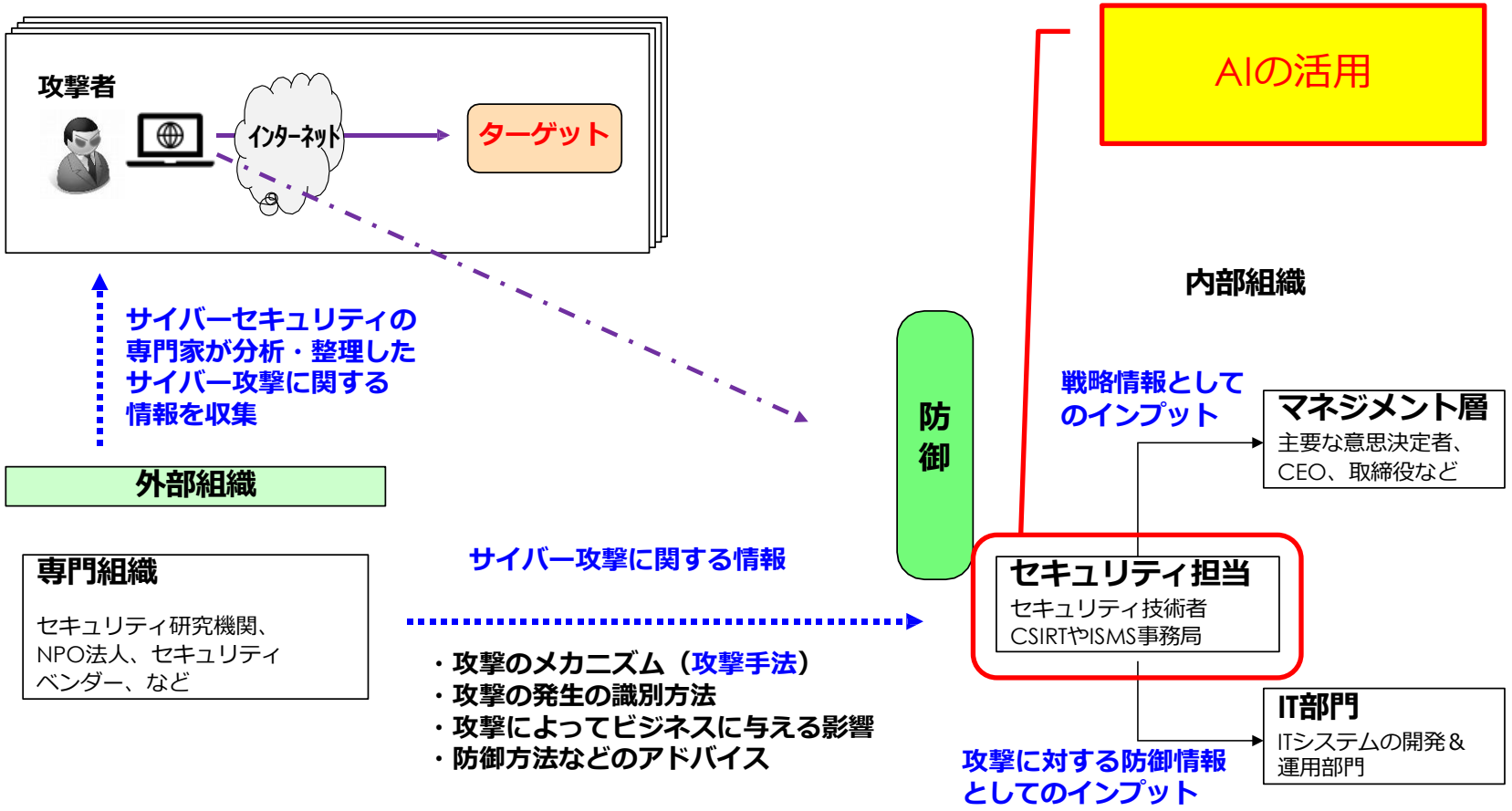
●AIが活用できるISMS事務局の仕事は、年間のマネジメントシステム活動の定常的な運用だけか？

○ISMS事務局には、情報セキュリティにおける司令塔の役割を持ち、AIを活用した脅威インテリジェンスの中核的な役割を期待する。

【SC27/WG1チームの主張】
AIは、ISMS事務局のマネジメント活動の補助だけでなく、脅威インテリジェンスの戦略的脅威分析にこそ活用すべき。

脅威インテリジェンスとは？(イメージ図)

2023年度テーマ１資料

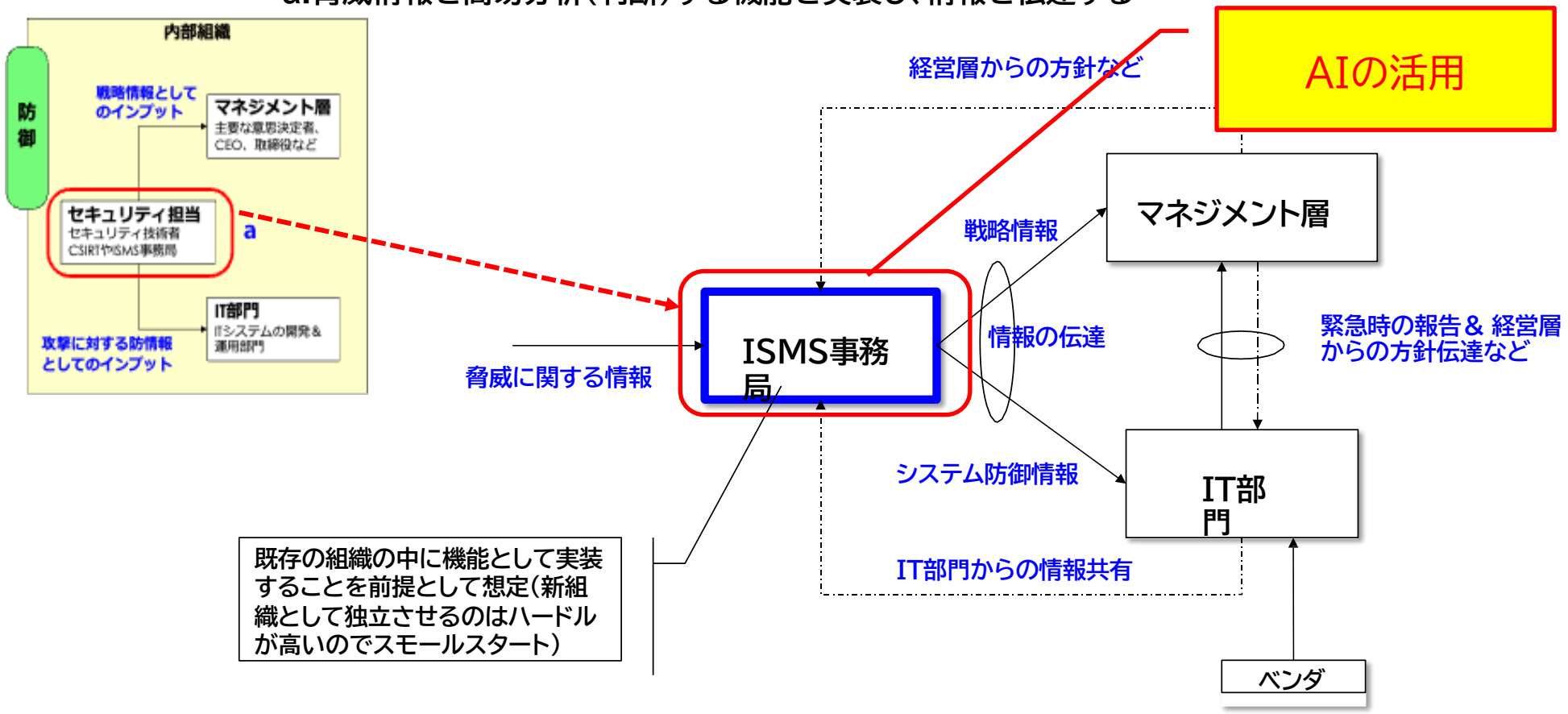


活用ポイント・・・a

2023年度テーマ１資料

参考情報

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



脅威インテリジェンスの体制構築の例

【参考：脅威インテリジェンスを役割別の層としたモデル】
1. ガバナンス層（経営・統制）：方針・資源・責任・優先度の決定
2. マネジメント層（制度・リスク管理）：ISMS・リスク管理・ルール整備
3. オペレーション層（技術・運用）：SOC/Blue Team、監視、防御、日常運用
4. インシデント対応層（CSIRT/PSIRT）：事案対応・再発防止・連携

●ISMS運用体制の例

【経営層】
└── CISO
　　├── ISMS管理責任者 ―（ISMS事務局）
　　├── セキュリティ運用（SOC）
　　│　　└── アナリスト／脆弱性管理／監視
　　├── IT運用（ネットワーク/クラウド/ID管理）
　　├── DevSecOps（開発・CI/CD・診断）
　　└── CSIRT（事案対応）

※出典：AIにISO/IEC27001/27002/27035,NIST CSF,NIST SP 800-61,27005など
　　複数規格の要点をまとめさせて作成したもの

AIは、敵でも味方でもない

AIはどちら側でも
利用される

攻撃側のAI活用が急激に進み、既に主要な作業工程をAIが担ったサイバー攻撃が行われているため、防御側もAIを活用し対抗しなければならない。ISMS事務局は、技術力の経験や知識をAIで補うことで、脅威インテリジェンスにおけるマネジメント層として脅威分析・情報収集を行い経営と ICT の橋渡しを担うことを検討すべき。

AI活用が望まれる脅威の特徴(ランサムウェアの例)

- 脅威アクターの“速度増幅”

  「侵入 → lateral movement(横展開) → 暗号化 → 流出初期侵入から横展開・暗号化」へ移る時間が大幅に短縮されている。

  - クラウド／SaaS／仮想化環境を狙い、「広範囲／高速スキャン → 標的化 → 被害実行」のサイクルを縮めている。
  - 生成AIや自動化ツールを使い、フィッシング文面・マルウェア作成・侵入経路発見などの工程を「より迅速かつ安価に」実施。
  - 侵入後、被害対象(例えば仮想化ホスト・サーバ・管理者アカウント)を迅速に特定し、短時間で暗号化や横展開を完了させる事例が増えている。脅威アクターの“速度増幅”

- この“速度増幅”に組織のISMS事務局もICT部門も対応が遅れている

  ⇒原因は「人の手の遅れ(Human latency)」と考えられる。この対応には、経営陣、ISMS事務局、ICT部門の3者が緊密な連携を取らなければならないが、2023年度テーマ1資料にもあるようにISMS事務局がキーポイントである。

AI活用の責任分界と対応の例

■【経営陣：戦略的インテリジェンス】
組織の置かれている状況をISMS事務局から報告を受け、戦略的インテリジェンス対応についてISMS事務局及びICT部門へ的確な指示を出す。

■【ISMS事務局：戦略的インテリジェンスと運用インテリジェンス】
組織が対処すべき脅威についてAIを使って分析し、戦略的脅威を経営陣に報告し対応の承認を得る。決定した脅威（例えば、ランサムウェア）対応についてICT部門に検討を指示すべき情報をAIを使って確認する。
ICT部門が実装するとした対策を費用対効果も含めてその有効性をAIを利用してレビュー・評価する。

■【ICT部門：運用インテリジェンスと戦術的インテリジェンス】
ISMS事務局及び経営陣からの情報や指示により、脅威（例：ランサムウェア）対策として「GuardDuty（脅威検出） → EventBridge（他のサービスへ自動的に連携） → Lambda（サーバレス実行環境） による自動隔離」などを検討し実装する。その際、効果的な対策の実装とその運用についてAIを活用する。対策の実装に当たっては、ISMS事務局に提案しレビューを受ける。

ISMSへの実装の観点