

生成AIで進化する、次世代のISMS運用の形

JNSA 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

2025年 12月5日

井崎 友博

はじめに

- 情報セキュリティマネジメントシステム（ISMS）は、ISO/IEC 27001を中心として2000年代初頭に国際的な認証制度として整備された。
- しかしその運用は、主として人手によるドキュメント整備・記録更新・内部監査・是正対応といった、労働集約的な活動に依存してきた。これにより、ISMSは形式的運用・定常業務化・属人化といった課題を内包するようになった。
- ISMSは「継続的改善」を前提とする制度であるが、その実施には膨大な情報整理と判断作業を要する。この構造は組織の成熟度や担当者の力量に強く依存し、運用の一貫性・再現性を確保することが難しい。

- 一方で、近年の人工知能（AI）、特に大規模言語モデル（LLM）の急速な発展により、自然言語で記述された情報資産・リスク文書を解析・生成できる技術的基盤が整いつつあり、従来人手に依存していた作業の一部を支援できる可能性を示している。
- こうした技術進化は、ISMSの運用を「人の経験と判断に基づく手作業」から、「データとモデルに基づく協働的判断」へと変革させうる。すなわち、ISMSの本質である「継続的改善」を、より動的かつ知的に支援する仕組みの萌芽であると考えている。

AIを活用し、事務局のISMS運用業務を支援できるか

- 特に「リスク特定」「リスク分析」の2領域を対象とする。
- 事務局を対象とする（現場担当者を対象としない）。
- 定量的な精度比較・分析・研究を目的とするのではなく、実例と知見の共有を目的とする（探索的な研究）。
 - そのため、何らかの真理を発見したり、強いエビデンスを示すものではない。

先行研究からわかること

2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

Work in Progress: Leveraging Large Language Models for Cybersecurity Compliance: A Pilot Study in ISO 27001 Audit Planning

1st Ahmed Salman
Department of Computer Science
University of Oxford
Oxford, UK
ahmed.salman@cs.ox.ac.uk

2nd Yara Alsiyat
Department of Computer Science
University of Oxford
Oxford, UK
yara.alsiyat@wolfson.ox.ac.uk

3rd Sadiq Creese
Department of Computer Science
University of Oxford
Oxford, UK
sadiq.creese@cs.ox.ac.uk

4th Michael Goldsmith
Department of Computer Science
University of Oxford
Oxford, UK
michael.goldsmith@worc.ox.ac.uk

Abstract—Cybersecurity compliance processes are often subjective and error-prone due to their reliance on manual documentation. This pilot study evaluates the potential of Large Language Models (LLMs) in cybersecurity compliance during the planning phase of ISO 27001 standard. Using a hypothetical telecommunications organization, we evaluated three tasks: Statement of Applicability generation, audit scope definition, and compliance checklist development, assessing Sonnet 3.5, ChatGPT 4.0, and Llama 3.1 via ordinal scoring and qualitative factors (e.g., scalability, skill coverage). Sonnet 3.5 consistently outperformed other models across all tasks, though all struggled with completeness and data assimilation. These findings validate LLMs' ability to streamline compliance workflows while highlighting key limitations that must be addressed for practical deployment.

1. Introduction

Cybersecurity compliance is essential for organizational assurance but faces persistent inefficiencies. Prior work [1] highlights three key challenges: a lack of environmental evidence, where documentary audits sometimes overlook real-time network insights (e.g., configuration logs); static approaches, slow to adapt to regulatory or threat changes; and human subjectivity, introducing variability into manual assessments. While automation has been proposed to mitigate these issues, such efforts have struggled with the extensive analysis required for vast, unstructured compliance data. Large Language Models (LLMs), with their ability to process unstructured formats, present a promising solution [1]. This paper presents a pilot study testing this approach within a telecommunications compliance context, focusing on the critical planning and scoping stage that provides a foundation for subsequent compliance steps like fieldwork, analysis, and reporting.

Planning and scoping in compliance activities require precision, domain-specific expertise, and considerable effort. As the foundational phase, effective planning en-

sures downstream audit accuracy and regulatory alignment, making it a key target for automation. Unlike sectors reliant on cloud providers, telecommunications still maintain complex, on-premises IT systems, offering a compelling testbed for compliance workflows. We adopted ISO 27001, a widely recognized standard across industries, for its structured approach and extensive resources [2]. Figure 1 depicts the general compliance life-cycle [3], presenting planning as the foundational stage evaluated here. To anchor our study, we created HelloPak, a hypothetical Mobile Network Operator (MNO). Figure 2 illustrates HelloPak's network, providing context for our experiments.

We targeted three planning tasks: Statement of Applicability (SoA) generation, audit scope definition, and checklist creation. Initially planned as a purely qualitative evaluation, we incorporated ordinal scoring, common in LLM assessments [4], [5], to rank output quality by relevance and completeness. Additionally, we used qualitative scoring to assess scalability, skill coverage, and change absorption. Unlike prior studies targeting specific compliance steps (e.g., policy analysis [6], [7]), this pilot study explores LLMs across the ISO 27001 planning phase. This dual approach offers practical insights into LLMs' operational utility in cybersecurity compliance workflows. As a novel pilot, it lays the foundation for broader exploration of subsequent stages in the compliance workflows. Next, we outline our methodology to evaluate these tasks and scoring methods in detail.

2. Methods

This pilot assesses three LLMs for the compliance planning stage: Sonnet 3.5 [8], Llama 3.1 [9] (both hosted on the Abacus AI platform), and ChatGPT 4.0 [10] (OpenAI platform), selected for their recency, availability, and benchmarking at the study's outset. Although newer LLMs have since emerged, our focus on operational insights ensures the study's relevance. Using multiple LLMs mitigates bias from any single model's weaknesses, enhancing the robustness of our observations. Access to these LLMs

© 2025, Ahmed Salman. Under license to IEEE.
DOI 10.1109/EuroSPW67616.2025.00046

351

- ISO/IEC 27001の計画段階（SoA作成・監査計画・チェックリスト生成）におけるLLMの有用性を実験的に検証した研究。
- Claude 3.5 Sonnet、ChatGPT-4o、Llama 3.1を比較した結果、Sonnetが最も高精度であったが、完全性不足やハリシネーション、スケーラビリティの課題が残る。
- 特に詳細で構造化されたプロンプト設計とデータ整備が成果を左右し、現時点では人間の監督を前提とした補助的利用が望ましいと結論づけている。

Salman et al., "Evaluating LLMs in ISO/IEC 27001 Planning Phase Tasks,"
IEEE EuroS&P Workshops, 2025.

Utrecht University
ICT STARTUPS

Automating ISO 27001 Consultancy and Auditing using AI: A Feasibility Study Based on Expert Interviews

Authors:
S.I. (Steven) Riasat (2562863)
C.E.W. (Mike) Brachten (6932983)
Supervisor:
Dr. R.L. (Slinger) Jansen
ORCID 0000-0003-1754-2984

December 8, 2023

- ISO/IEC 27001 監査・コンサル業務へのAI導入可能性を専門家6名へのインタビューで検証した。
- 監査プロセス中では特に報告書作成（評価フェーズ）の負荷が大きく、生成AIはその効率化に有望と結論づけた。
- 一方で**精度・機密性・人の判断の欠如が課題**とされ、人間中心の補助的活用が望ましいとした。

S. I. Riasat and C. E. W. Brachten, "Automating ISO 27001 Consultancy and Auditing using AI: A Feasibility Study Based on Expert Interviews," Preprint, Utrecht University, Dec. 2023.

当研究のテーマ

研究会メンバーに「困っていること」アンケートを実施

- 篠条4～10ならびに附属書Aの各項目について、下記の質問を実施。

日々のISMS運用において、課題や負担に感じる点を、すべて選択してください。

アンケート結果をもとに、研究対象として3つのテーマを選定

#	課題	規格の章	票数	研究対象
1	情報セキュリティリスクを適切に特定すること	6章	12	✓
2	ログ取得・監視	附属書A	11	<div style="border: 1px solid black; padding: 5px; display: inline-block;">除外理由：すでに技術的な解決策（ログ管理ツール）がありそう</div>
3	リスクアセスメントの結果に対し、一貫性・妥当性・比較可能性を担保すること	6章	10	✓
3	課題や利害関係者のニーズをもれなく整理すること	4章	10	
5	年間計画を策定し、計画通りに実行（必要に応じて変更管理）すること	8章	9	
5	供給者・クラウドサービスの管理	附属書A	9	
5	トップマネジメントに、リーダーシップやコミットメントを発揮いただくこと	5章	9	
5	技術的ぜい弱性の管理	附属書A	9	

事前準備 1：仮想的な資産台帳

- ある会社の「情報システム部」を想定した仮想的な資産台帳を用意。

資産名	カテゴリ	責任者	主管部門	機密分類	保管場所	利用可能な範囲
サーバ設定情報	情報	山田花子	情報システム部	機密	ファイルサーバ	情報システム部
ネットワーク図	情報	山田花子	情報システム部	機密	ファイルサーバ	情報システム部
勤怠管理システム	ソフトウェア	山田花子	情報システム部	社外秘	クラウド	全従業員
MDM	ソフトウェア	山田花子	情報システム部	機密	クラウド	情報システム部
ノートPC	ハードウェア	木村二郎	情報システム部	社外秘	個人管理	全従業員
スマートフォン	ハードウェア	山田花子	情報システム部	機密	個人所有	全従業員
ファイルサーバ	ハードウェア	田中太郎	情報システム部	機密	サーバルーム	情報システム部

事前準備2：仮想的なリスク台帳

- ある会社の「情報システム部」を想定した仮想的なリスク台帳を用意。
- リスクアセスメントは資産ベースで行われていることを想定。

資産名	リスク	発生可能性	影響度
ファイルサーバ	マルウェアの感染による暗号化・情報漏えい	中	高
ファイルサーバ	アクセス権限の設定ミスによる情報漏えい	高	高
ファイルサーバ	老朽化や過負荷によるハードウェア故障	低	高
ファイルサーバ	バックアップ失敗によるデータ消失	低	高
ファイルサーバ	災害や停電による長時間のサービス停止	低	中
ファイルサーバ	内部不正による機密ファイル改ざん	低	中
ノートPC	盗難・紛失による情報漏えい	中	高
ノートPC	OSやアプリの未更新によるマルウェア感染	中	高
ノートPC	公共Wi-Fi利用時の盗聴やなりすまし	中	中
ノートPC	パスワード使い回しによるアカウント乗っ取り	高	高
ノートPC	物理的損傷による業務停止	低	中
ノートPC	不正USB接続によるデータ持ち出し	低	中
...

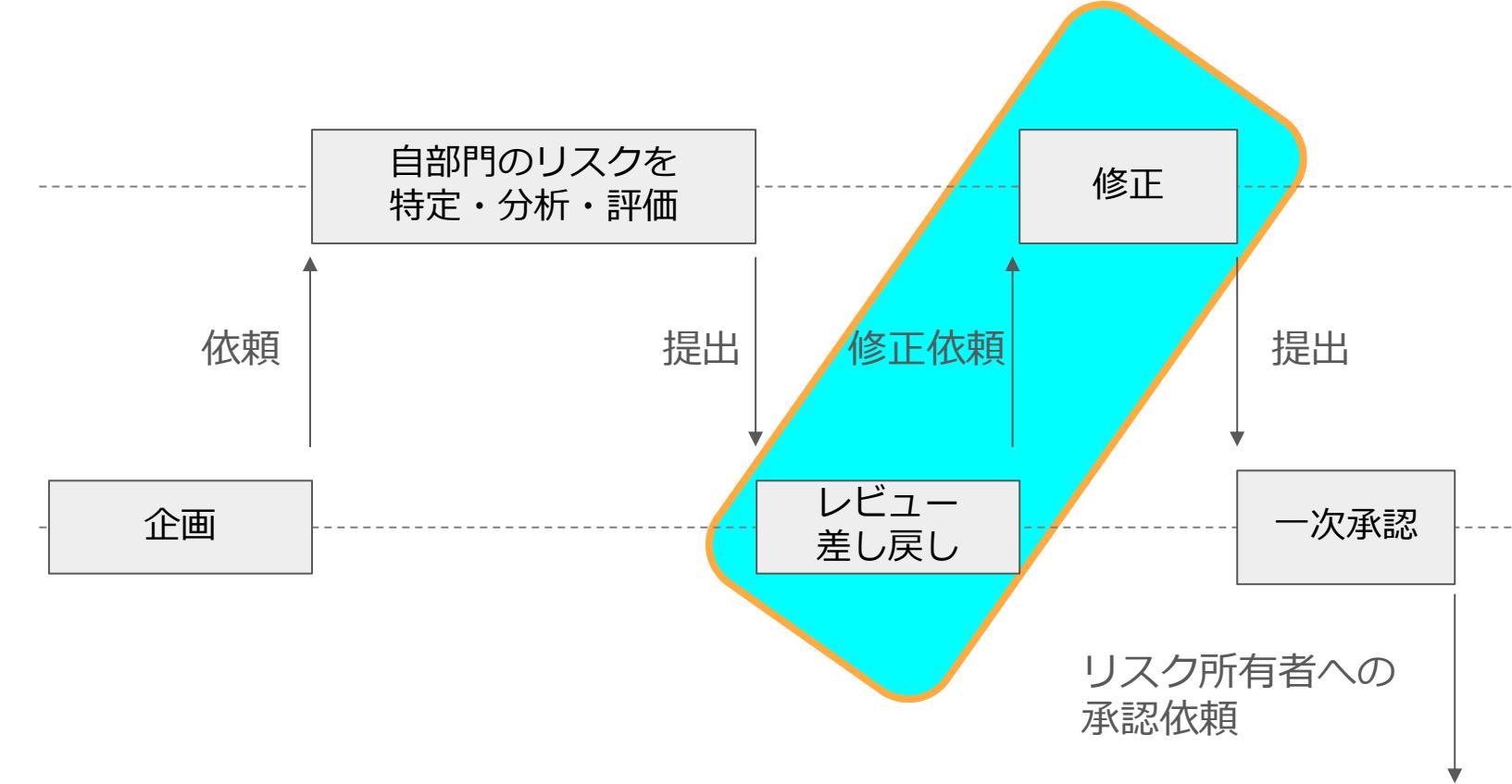
テーマ1： 情報セキュリティリスクを適切に特定する

- 現場レベルで特定したリスクに**致命的な抜け漏れ**があるかもしれない、特定方法次第では、現場が特に**危険視しているリスクが特定しにくい**ケースもある。
- どうしても部署ごとに**検討の深さ**が異なってしまう
- 必ずしも網羅的に特定できているわけではなく、なかなかリスクが思いつきづらかったり、リスクは把握していても担当者の判断で特定しないなど、一覧上では**抜け漏れ**が生じやすい状態も生まれているように感じます。
- **漏れ**が中心、初年度特定してから2年目以降ほぼ**変わりがない**ところ←大問題
- 何も考えずに手続きを実施すればよいとの判断で現場が動いていることが多い。少なくともリスクを適切に特定出来るようにしないと形式的な取り組みとなってしまう

一般社員
1線

各部の担当者
1.5線

事務局
2線



- 下記の内容をプロンプトとして、ChatGPTに入力。
 - プレースホルダー箇所 ({{}}) は、CSVデータとして貼り付け。

あなたは、企業に対して情報セキュリティリスクアセスメントの支援を行うコンサルタントです。クライアントが保有している以下の資料を元に、指定された資産のリスク特定を行ってください。

資料

- クライアントの資産リスト : {{asset_list}}
- クライアントのリスクリスト : {{risk_list}}

リスク特定を行う対象資産

{{asset_name}}

依頼事項

1. 資産リストから対象資産を見つけ、その資産の概要を把握してください。
2. リスクリストから対象資産に紐づくリスクを見つけ、すでに特定されているリスクを把握してください。
3. リスクリストに特定が漏れているリスクを、最大5つまで提案してください。リスクは20文字以内で端的に表現してください。

出力フォーマット

漏れているリスクを、プレーンテキストかつ箇条書きで出力してください。
それ以外の情報出力は行わないでください。

結果 - サーバ設定情報（情報資産）

リスクリストの記載	試行1	施行2	施行3
アクセス権限の不備による機密情報流出	・権限昇格で設定変更	・不適切なファイル保管	
平文パスワード記載による不正ログイン			
バージョン管理不足で誤設定を展開			
バックアップ未取得による情報喪失			
悪意ある改ざんに気付かず適用			
マルウェア感染でファイル暗号化・閲覧不能			
(誤設定)	・誤設定による通信障害 ・更新漏れによる脆弱性露出 ・不正な外部アクセス許可 ・認証情報の誤配置	・誤った設定でサービス停止	・設定情報の権限誤設定 ・誤操作による設定消失
(コピー・送信)		・設定ファイルの不正コピー ・誤送信による情報漏えい	・設定情報の不正持ち出し
(バックアップ)		・バックアップデータの改ざん	・バックアップデータの破損
(その他)	・設定変更による互換性問題		

結果 - 勤怠管理システム (ソフトウェア資産)

リスクリストの記載	試行1	施行2	施行3
クラウドサービス停止による勤怠入力不能		・API過負荷による応答遅延	
脆弱なAPI認証による従業員データ漏えい			
不正アクセスによる勤怠記録改ざん		・社内不正アクセスによるデータ改ざん ・認証情報のフィッティング被害	・外部連携APIの不正利用による情報漏えい
SaaSアカウントの多要素認証未設定			
ベンダ側設定変更によるデータ消失	・定期的な脆弱性診断不足		・プログラム適用ミスによる不具合 ・セキュリティパッチの未適用
ID基盤障害によるシングルサインオン失敗			
(誤操作)	・従業員教育不足による誤操作 ・ユーザ権限管理不備	・誤った勤怠承認による混乱	・従業員誤操作によるデータ破損
(暗号化)		・暗号化通信の不備による情報漏えい	
(ログ)	・ログ監視不備による不正検知遅れ		・ログ管理不備による不正行為見逃し
(その他)	C		

結果 - ファイルサーバ (ハードウェア資産)

リスクリストの記載	試行1	施行2	施行3
マルウェアの感染による暗号化・情報漏えい		・外部からの不正アクセス	・外部攻撃によるデータ改ざん
アクセス権限の設定ミスによる情報漏えい			
老朽化や過負荷によるハードウェア故障			
バックアップ失敗によるデータ消失			
災害や停電による長時間のサービス停止	・電源供給の単一故障点		
内部不正による機密ファイル改ざん			
(物理的な攻撃)	・不正なUSBデバイス挿入		・不適切な物理アクセス管理
(パッチマネジメント)	・ファームウェア未更新による脆弱性	・ソフトウェアアップデート不足	・システムアップデートの遅延
(ファシリティ)	・空調故障による過熱リスク	・冷却システムの故障	・冷却システム故障による過熱
(監視・監査)	・定期的なログ監視不足による異常検知遅れ	・設定変更のログ管理不足	・定期監査の未実施

- 一定、特定が漏れているリスクを洗い出すことができた。
 - ただし、試行によってばらつきが多く、安定した値を得ることが難しい。
- 過去のインシデント情報を与えることで、LLMによる提案に補助線を与えることが可能では？

仮想的なインシデント台帳

- 資産を元に、仮想的なインシデント台帳を作成。

タイトル	概要
PCの置き忘れ	ノートPCを電車の中に置き忘れた。その後鉄道会社に問い合わせて回収。
サーバールーム鍵の紛失	ファイルサーバを設置したサーバールームの鍵を委託業者が紛失し、一定時間入退室管理が機能しなかったため緊急でシリンド交換を実施。
個人クラウド同期による資料流出	ノートPCで私用のクラウドストレージ同期が有効化されており、社外秘の設計書が自動的に個人アカウントへアップロードされたことが判明。
退職者アカウント残存による勤怠改ざん	勤怠管理システムで退職者のIDが無効化されておらず、第三者がその資格情報を用いて勤怠データを書き換えた形跡が見つかった。
MDM監査ログの欠落	MDM管理コンソールで監査ログ保存期間の設定が誤っており、不正な端末登録操作が行われた時刻のログが自動削除され調査が難航。
設定資料の紙媒体放置	サーバ設定情報を印刷した資料が会議室に放置され、来訪者が内容を閲覧できる状態だったため即時回収と廃棄を行った。
オンライン会議中のネットワーク図露出	外部ベンダーとのオンライン会議で誤って全社ネットワーク図が画面共有され、会議録画にも機密構成が残ったため削除依頼を行った。

- 下記の内容をプロンプトとして、ChatGPTに入力。
 - プレースホルダー箇所 ({{}}) は、CSVデータとして貼り付け。

あなたは、企業に対して情報セキュリティリスクアセスメントの支援を行うコンサルタントです。クライアントが保有している以下の資料を元に、指定された資産のリスク特定を行ってください。

資料

- クライアントの資産リスト : {{asset_list}}
- クライアントのリスクリスト : {{risk_list}}
- クライアントの過去発生したインシデントのリスト : {{incident_list}}

リスク特定を行う対象資産

{{asset_name}}

依頼事項

1. 資産リストから対象資産を見つけ、その資産の概要を把握してください。
2. リスクリストから対象資産に紐づくリスクを見つけ、すでに特定されているリスクを把握してください。
3. リスクリストに特定が漏れているリスクを、**過去に発生したインシデントのリストを参考に**、最大3つまで提案してください。リスクは20文字以内で端的に表現してください。

出力フォーマット

漏れているリスクを、プレーンテキストかつ箇条書きで出力してください。
それ以外の情報出力は行わないでください。

結果 - サーバ設定情報（情報資産） / 印刷した設定情報を会議室に放置したことがあった

元々の記載	試行1	施行2	施行3
アクセス権限の不備による機密情報流出		<ul style="list-style-type: none">・設定資料の不適切な共有・設定情報の個人クラウド同期	<ul style="list-style-type: none">・個人クラウド同期による情報流出・誤共有による機密情報露出
平文パスワード記載による不正ログイン			
バージョン管理不足で誤設定を展開			
バックアップ未取得による情報喪失			
悪意ある改ざんに気付かず適用			
マルウェア感染でファイル暗号化・閲覧不能			
(紙媒体)	<ul style="list-style-type: none">・紙媒体の放置による情報漏えい・印刷物の回収不足による流出	<ul style="list-style-type: none">・紙媒体放置による情報漏えい	<ul style="list-style-type: none">・紙媒体放置による情報漏えい
(コピー・送信)	<ul style="list-style-type: none">・誤送信による外部流出		

結果 - 勤怠管理システム（ソフトウェア資産） / 退職者のアカウント残りがあった

元々の記載	試行1	施行2	施行3
クラウドサービス停止による勤怠入力不能			
脆弱なAPI認証による従業員データ漏えい			
不正アクセスによる勤怠記録改ざん			
SaaSアカウントの多要素認証未設定			
ベンダ側設定変更によるデータ消失		・ベンダー設定ミスによる情報漏えい	・ベンダ設定ミス露出
ID基盤障害によるシングルサインオン失敗			
(退職者アカウント)	・退職者アカウントの無効化漏れ	・退職者アカウント残存による不正アクセス	・退職者アカウント残存
(ログ)	・誤設定による監査ログ欠落		
(その他)	・クラウドストレージ同期の不正利用	・個人クラウド同期によるデータ流出	・個人クラウド同期

結果 - ファイルサーバ（ハードウェア資産） / サーバルームの鍵紛失があった

元々の記載	試行1	施行2	施行3
マルウェアの感染による暗号化・情報漏えい			
アクセス権限の設定ミスによる情報漏えい			
老朽化や過負荷によるハードウェア故障			
バックアップ失敗によるデータ消失			
災害や停電による長時間のサービス停止			
内部不正による機密ファイル改ざん			
(サーバルーム)	<ul style="list-style-type: none">・鍵紛失による物理的アクセス	<ul style="list-style-type: none">・サーバルームの鍵紛失	<ul style="list-style-type: none">・サーバルーム鍵の紛失による不正アクセス・委託業者のミスによる物理セキュリティ低下
(その他)	<ul style="list-style-type: none">・設定資料の紙媒体放置・ネットワーク図の意図せぬ露出	<ul style="list-style-type: none">・設定資料の紙媒体放置・オンライン会議での図面露出	<ul style="list-style-type: none">・設定資料の紙媒体放置による情報漏えい

- 過去のインシデント情報を与えることで、一定安定した結果を得ることができる。
- 一方で、まだインシデントとして顕在化していないリスクを見逃していないかは考慮が必要。

- インシデントの代わりに「情報セキュリティ10大脅威」の情報を与えることでも、出力を安定させることができた。
- 情報資産そのものに対しては、リスクの特定のばらつきが多くなったり、意味が掴めないリスクが提案されることが多かった。おそらく、その会社固有の情報である（AIがコンテキストを理解できない）からだと考えられる。そのため、情報資産そのものより、支援資産（ハードウェア、ソフトウェア、ネットワーク、拠点等）に対してアセスメントを行う手法と相性が良いと考えられる。
- インシデントリストがそもそもない（集約するのが難しい）という意見もあった。

提出いただいたリスクアセスメントの結果について、ISMS事務局にてレビューしたところ、気になる点がいくつかございました。

ご確認の上、必要であればリスクアセスメントシートに記入いただき、再提出いただけますよう、よろしくお願ひいたします。

なお、以下の提案は、当社内で過去発生したインシデントに基づいてご案内しています。

「サーバ設定情報」について

- ・紙媒体の情報を放置してしまうリスクの特定は不要でしょうか？

「勤怠管理システム」について

- ・退職者のアカウントに関するリスクの特定は不要でしょうか？

「ファイルサーバ」について

- ・サーバルームのカード管理や不正侵入に関するリスクの特定は不要でしょうか？

インシデントの発生を未然に防ぐために、ご協力いただけますと幸いです。
以上、どうぞよろしくお願ひいたします。

テーマ2： リスクアセスメントの結果に対し、 一貫性・妥当性・比較可能性を担保する

- 各部署で任命したISMS委員により取り扱うデータごとでリスクアセスメントを実施いただいているが、どうしても**部署ごとに検討の深さが異なってしまう**
- 一貫性・妥当性・比較可能性については、発生可能性や影響度などを数値化し一定整合が取れるようにはしているものの、それでも**その基準を必ずしも同じ理解するわけではない**というバラつきは生じやすいように感じます（特に影響度については人によって判断がぶれやすいように見受けられます）。
- 正直部署ごとでブレがあってもいいと思うが（承認者マターなため）どうしても**担当や部署によってブレがある**リスクアセスメント結果になっている点
- 横並びで見た時に、**部門間の一貫性を担保する**のも、かなり骨の折れる作業（事務局負担の大きい作業）になっている。

繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。

JIS Q 27001:2023 6.1.2 b)

一貫性 (consistency): 同じリスクについて、異なる人が実施した場合、あるいは同じ人が異なる機会に同じ状況で実施した場合でも、類似した結果が得られること。

比較可能性 (comparability): リスクアセスメント基準を定義することで、異なるリスクに対するアセスメント結果を、同等のリスクレベルを表す場合に比較可能にすること。

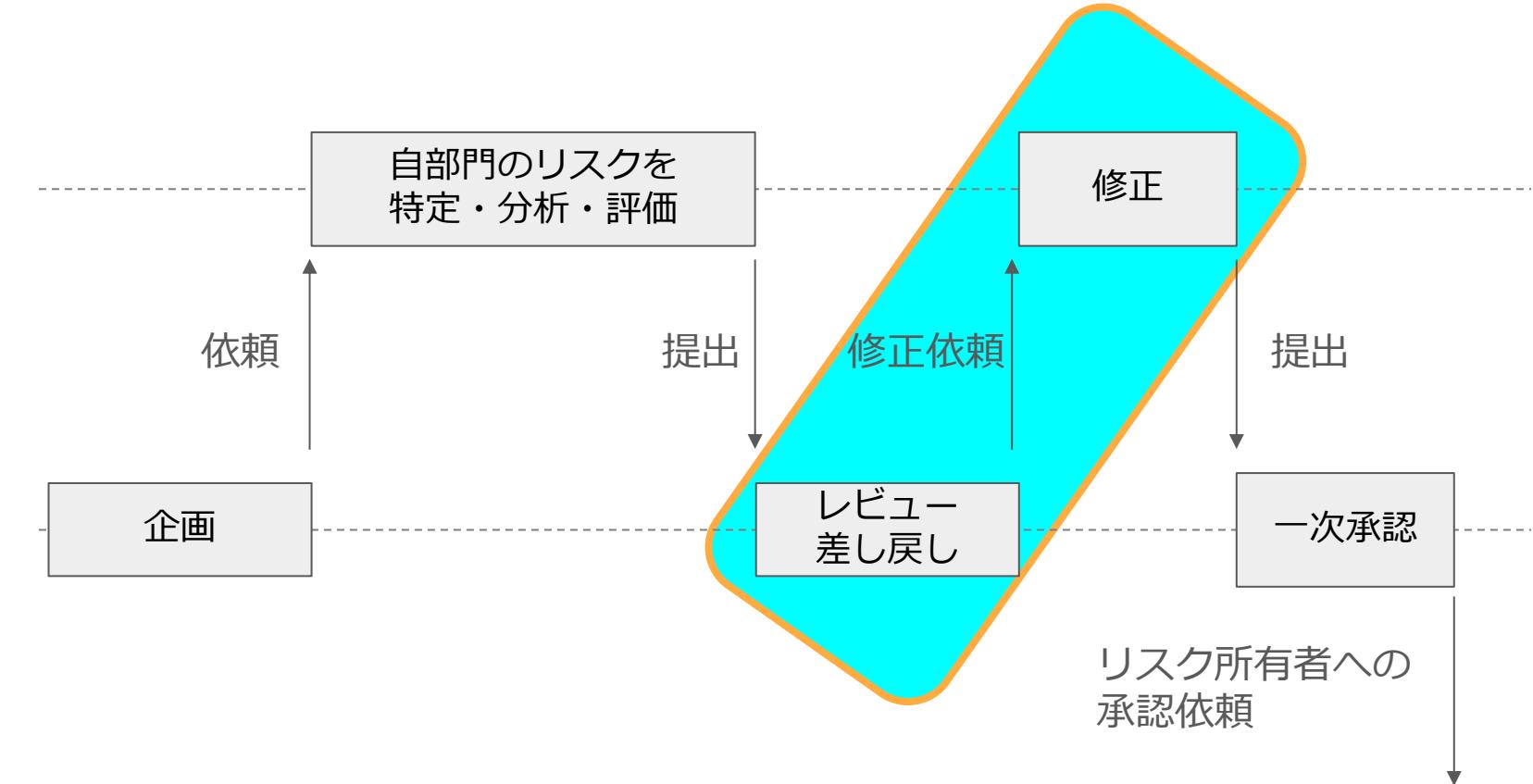
妥当性 (validity): アセスメントが現実にできる限り正確に一致する結果を生み出すこと。

ISO/IEC 27005:2022 6.5 より、井崎訳

一般社員
1線

各部の担当者
1.5線

事務局
2線



- 下記の内容をプロンプトとして、ChatGPTに入力。
 - プレースホルダー箇所 ({{}}) は、CSVデータとして貼り付け。

あなたは、企業に対して情報セキュリティリスクアセスメントの支援を行うコンサルタントです。
クライアントが保有している以下の資料を元に、以下を担保したリスク分析を実施します。

- 一貫性 (consistency): 同じリスクについて、異なる人が実施した場合、あるいは同じ人が異なる機会に同じ状況で実施した場合でも、類似した結果が得られること。
- 比較可能性 (comparability): リスクアセスメント基準を定義することで、異なるリスクに対するアセスメント結果を、同等のリスクレベルを表す場合に比較可能にすること。
- 妥当性 (validity): アセスメントが現実にできる限り正確に一致する結果を生み出すこと。

資料

- クライアントの資産リスト : {{asset_list}}
- クライアントのリスクリスト : {{risk_list}}

依頼事項

1. 資産リストを読み、各資産の概要を把握してください。
2. リスクリストを読み、各リスクの「発生可能性」および「影響度」を把握してください。
3. 上述した「一貫性」「比較可能性」「妥当性」の観点から、誤っていると考えられる「発生可能性」もしくは「影響度」を3つまで提示してください。

出力フォーマット

(省略)

結果

	試行1	試行2	試行3	試行4	試行5
1	ファイルサーバ,内部不正による機密ファイル改ざん 発生可能性 低→中	サーバ設定情報, 平文パスワード記載による不正ログイン 発生可能性 低→高	サーバ設定情報, アクセス権限の不備による機密情報流出 発生可能性 中→高	ノートPC,OSやアプリの未更新によるマルウェア感染 発生可能性 中→高	ノートPC,公共Wi-Fi利用時の盗聴やなりすまし 発生可能性 中→高
2	ノートPC,公共Wi-Fi利用時の盗聴やなりすまし 影響度 中→高	ノートPC, OSやアプリの未更新によるマルウェア感染 発生可能性 中→高	ネットワーク図,添付の管理情報から内部IP範囲が露出 影響度 中→高	スマートフォン,QRコードやSMSを悪用したフィッキング修正すべき項目: 影響度 高→中	スマートフォン,脱獄・ルート化によるセキュリティ設定無効化 発生可能性 低→中
3	MDM,デバイスインベントリの不整合による未管理端末放置 影響度 中→高	ネットワーク図, 添付の管理情報から内部IP範囲が露出 影響度 中→高	ネットワーク図,旧構成のまま更新されず誤った対策判断 発生可能性 中→高	勤怠管理システム,クラウドサービス停止による勤怠入力不能 発生可能性 中→低	サーバ設定情報,平文パスワード記載による不正ログイン 影響度 高→中

- 施行ごとにはらつきがかなり大きい。そのため、妥当な提案かどうかを判断することができない。
→ 最新の「情報セキュリティ10大脅威 2025」の情報を与えることで、LLMによる提案に補助線を与えることが可能では？

ChatGPTを利用したリスク特定

- 下記の内容をプロンプトとして、ChatGPTに入力。
 - プレースホルダー箇所 ({{}}) は、CSVデータとして貼り付け。

あなたは、企業に対して情報セキュリティリスクアセスメントの支援を行うコンサルタントです。クライアントが保有している以下の資料を元に、以下を担保したリスク分析を実施します。

- 一貫性 (consistency): 同じリスクについて、異なる人が実施した場合、あるいは同じ人が異なる機会に同じ状況で実施した場合でも、類似した結果が得られること。
- 比較可能性 (comparability): リスクアセスメント基準を定義することで、異なるリスクに対するアセスメント結果を、同等のリスクレベルを表す場合に比較可能にすること。
- 妥当性 (validity): アセスメントが現実にできる限り正確に一致する結果を生み出すこと。

資料

- クライアントの資産リスト : {{asset_list}}
- クライアントのリスクリスト : {{risk_list}}
- **最新のセキュリティ脅威:{{threat_list}}**

依頼事項

1. 資産リストを読み、各資産の概要を把握してください。
2. リスクリストを読み、各リスクの「発生可能性」および「影響度」を把握してください。
3. **最新のセキュリティ脅威をもとに**、上述した「一貫性」「比較可能性」「妥当性」の観点から、誤っていると考えられる「発生可能性」もしくは「影響度」を3つまで提示してください。

出力フォーマット

(省略)

Copyright (c) JNSA Japan ISMS User Group. 2025

結果

	試行1	試行2	試行3	試行4	試行5
1	ファイルサーバ、マルウェアの感染による暗号化・情報漏えい 発生可能性 中 → 高	ノートPC、OSやアプリの未更新によるマルウェア感染 発生可能性 中 → 高	ファイルサーバ、マルウェアの感染による暗号化・情報漏えい 発生可能性 中 → 高	ファイルサーバ、マルウェアの感染による暗号化・情報漏えい 発生可能性 中 → 高	ファイルサーバ、マルウェアの感染による暗号化・情報漏えい 発生可能性 中 → 高
2	MDM、サプライチェーンや委託先を狙った攻撃 影響度 中 → 高	勤怠管理システム、SaaSアカウントの多要素認証未設定 発生可能性 中 → 高	スマートフォン、モバイルマルウェア感染による個人情報流出 発生可能性 中 → 高	勤怠管理システム、脆弱なAPI認証による従業員データ漏えい 発生可能性 低 → 中	ノートPC、OSやアプリの未更新によるマルウェア感染 発生可能性 中 → 高
3	勤怠管理システム、脆弱なAPI認証による従業員データ漏えい 発生可能性 低 → 中	サーバ設定情報、平文パスワード記載による不正ログイン 影響度 高 → 中	サーバ設定情報、バージョン管理不足で誤設定を展開 影響度 中 → 高	ノートPC、OSやアプリの未更新によるマルウェア感染 影響度 中 → 高	スマートフォン、QRコードやSMSを悪用したフィッシング 影響度 高 → 中

- 「情報セキュリティ10大脅威 2025」の情報を与えることで、ある程度安定した結果を得ることができた。
- ただし「発生可能性の修正」が多いため、影響度について良い結果を得るための方法は模索する必要がある。

- 過去のインシデントに関する情報源として含めていたが、インシデントは過去の結果であり、それに対する是正処置が取られている今、参考にすべき情報ではないという意見があり、インプットからは除外した。
- そもそも、リスク基準について、各部の担当者とコミュニケーションが取れていれば、このような「一貫性・妥当性・比較可能性がブレる」ことはないという意見もあった。
- 最新の情報セキュリティ対策・管理策の情報はインターネット上に多く出回っているため、リスク対策の提案まで行うと、より良い出力が得られるのではないかという意見もあった。

提出いただいたリスクアセスメントの結果について、ISMS事務局にてレビューしたところ、気になる点がいくつかございました。

ご確認の上、必要であればリスクアセスメントシートに記入いただき、再提出いただけますよう、よろしくお願ひいたします。

なお、以下の提案は、IPAが公表する「セキュリティ10大脅威」に基づいてご提案差し上げています。

「マルウェアの感染による暗号化・情報漏えい（ファイルサーバ）」について

最新のセキュリティ脅威ランキングで「ランサム攻撃による被害」が1位にランクインしており、ランサムウェアによる脅威が増加しています。特にファイルサーバはランサムウェアのターゲットになりやすいため、発生可能性を「高」にしておく必要はないでしょうか？

「OSやアプリの未更新によるマルウェア感染（ノートPC）」について

最新のセキュリティ脅威として「システムの脆弱性を突いた攻撃」が挙げられており、脆弱性を悪用した攻撃が増加しています。特に、脆弱性が発見されてから攻撃が発生するまでの時間が短縮されていることから、OSやアプリの更新が遅れることで攻撃の対象となる可能性は高く、発生可能性を「高」としておく必要はないでしょうか？

インシデントの発生を未然に防ぐために、ご協力いただけますと幸いです。
以上、どうぞよろしくお願ひいたします。

まとめと今後の展望

- ChatGPTは安定した出力を得ることが難しく、繰り返し一貫性のあるリスクアセスメントを実現することには課題が残る。
 - なお、OpenAI社が提供するAPIなどを活用することで、回答内容に一貫性・安定性をもたせることができる（temperatureの設定）。
- 今回紹介した活用方法は、あくまで日々のISMS運用における補助的なツールにとどまり、人間によって行われる作業を代替できるレベルではない。しかし、AIのレベルは日に日に向上しているため、今後はさらなる品質・精度の向上が期待できる。

- 当研究では、OpenAI社が提供する、ChatGPTインターフェイスにおいて、GPT-4o モデルを利用した。なお、ISMS事務局の皆さんのが特別な工夫なく容易に取り組んでいただけるように、いわゆる「systemプロンプトの利用」や「fine tuning」などは実施していない。これらの活用は今後の課題である。
- 本研究はあくまで探索的な研究であり、統計的な有意性を担保しているものではない。また、データ量も十分ではないため、データが増えたときに、品質や性能が不十分になる可能性がある。
- 実データを利用する場合には、AIの学習に利用されないか、利用規約などを事前に確認しておくことも重要である。

ISMSのAI/DX化が進む中で、 ISMS事務局にとっての必要なスキルとはなにか？

今まで必要とされてきたもの

- 規程や手順書の整合性のチェック、体裁の調整。
- 機械的な監査チェックリストの作成業務。
- 年次の各部への棚卸し依頼業務。
- 証跡収集作業。

より必要になってくるもの

- AIの知見。プロンプティング。
- トップマネジメントやステークホルダーとのコミュニケーションや合意形成。
- 結果に対する説明責任。

