

Mindset for Information Security with AI



AI活用における 情報セキュリティ 意識レベル診断

既存の常識を覆す、生成AI時代の
絶対的最適解「MSIS/AI」

知識(建て前)から、本音の意識(Cognitive Risk)の可視化へ。

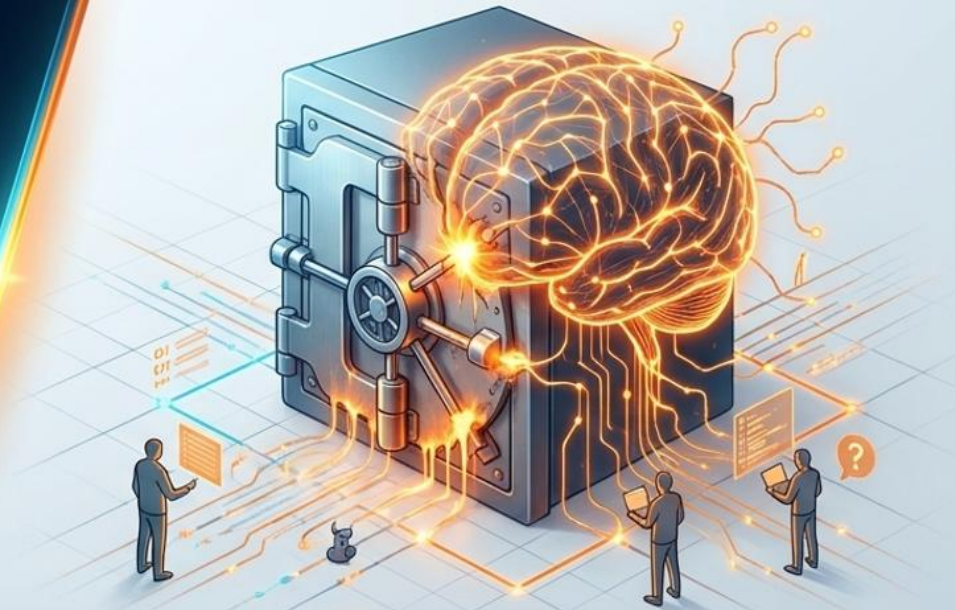
株式会社スクウェイブ

従来と次元が異なるインパクト

従来のセキュリティ対策



生成AIがもたらす新たな脆弱性



タイパ・効率化の強烈な誘惑

手でやると3時間かかる作業が、プロンプトを投げれば3秒で終わる。この強烈な成功体験が規律を容易に上書きする。



「会話型UI」による心理的無防備さ

親しみやすさがAIを「安全なアシスタント」と錯覚させ、機密情報を無意識に打ち明けてしまう。



無批判な依存とハルシネーションの軽視

「AIが言うなら正しい」という責任転嫁。ファクトチェックの手間を惜しむ、人間の根源的な怠惰。



いざという時の本音が肝心



手法

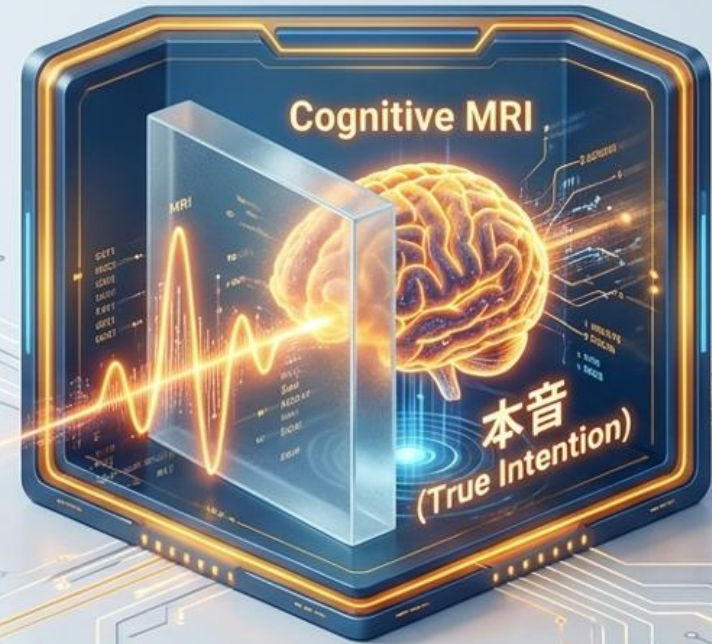
「社内規定に違反するAI利用は控えるべきですか？ (Yes/No)」

結果

顕在化した知識の確認のみ。正解が明白なため、全員が「Yes」と回答する。

致命的欠陥

知識（知っているか）と意識（どう行動するか）の決定的なギャップを測れない。



手法

状況判断を通じた潜在意識の測定。

結果

「業務のためなら仕方ない」「本当は自分もやりかねない」という潜在的な受容度（本音）を定量化。

圧倒的価値

実際の行動リスクを正確に予測し、事前に対策を打つことが可能。

本音が分かる

建て前を無効化する心理的ハック：「第三者投影法」

Scenario Box



状況：営業のCさんは、提案に急を要したため、未許可の生成AIに競合の製品パンフレットを読み込ませ比較表を作成。「公開情報ベースのAIアウトプットであり、このスピードこそAIの価値だ」と主張している。

あなたは、このCさんの行動・意見にどの程度賛同できますか？

1. 全く賛同できない

4. どちらとも言えない

7. 完全に賛同できる

投影効果

自身の行動として問われると働く「防衛機制（建て前）」を排除。

受容度の定量化

客観的立場で他者をジャッジさせることで、回答者自身の「リスクへの心理的ハードルの低さ（＝本音）」を正確に炙り出す。

適度な質問数（構造）

究極の黄金比率:「BEST MIX 25」

設問疲労を防ぎつつ、過去から未来までの全脅威を網羅する絶対的最適解。

AI活用リスク(14問)

生成AI普及期の新たな脆弱性を完全捕縛。
シャドーAIからハルシネーションまで、最先端の認知的死角を突く。

14

25

11

基幹リスク・IPA10大脅威(11問)

絶対に守り抜くべきセキュリティの基礎。
サプライチェーン攻撃、ランサムウェア、内部不正など、従来型の致命的脅威も死守。

AIの利便性に浮かれる組織の足元をすくう
「最新の間隙」と「基本的な油断」を、一網打尽にする唯一の質問体系。

具体的な質問数は協議の上、決定します。25問は推奨質問数であり、常に25問とは限りません。
※スクウェア社内では毎年最新のトレンドを踏まえて100問程度の標準ケースを更新しています。
※対象組織に適合する問題を選別提案します。

意識すべきAIの4大脅威

1. 機密情報・個人情報の流出(シャドーAI)



“「学習オプトアウトの確認より、目の前の業務完了が優先」
「社内資料なら個人情報さえ伏せれば大丈夫だろう」”

(本音の油断)

2. ファクトチェックの放棄・鵜呑み(ハルシネーション)



“「堂々と回答しているから合っているはず」「自分で調べる時間がないからAIを信じたい」という責任転嫁。”

(本音の油断)

3. 外部攻撃への無警戒(プロンプトインジェクション等)



“「便利な新プラグインは早く試したい」巧妙化するディープフェイクやフィッシングに対する認知的防御力の低下。”

(本音の油断)

4. 著作権・権利侵害・倫理的リスク



“「AIが生成したから自分のオリジナル」「みんなやっているから訴えられるわけがない」という無知と軽視。”

(本音の油断)

無視できない従来脅威

AIが新しいトレンドであっても、最終的な侵入経路は「人間の基本的な隙」にある。

サプライチェーン攻撃

関連会社や取引先を装った
巧妙なアプローチへの耐性

BECとランサムウェア

非日常的な要求や
緊急事態を装う攻撃への
冷静な判断力

認証バイパス・MFA

利便性を優先した
認証プロセスの形骸化・
迂回リスク

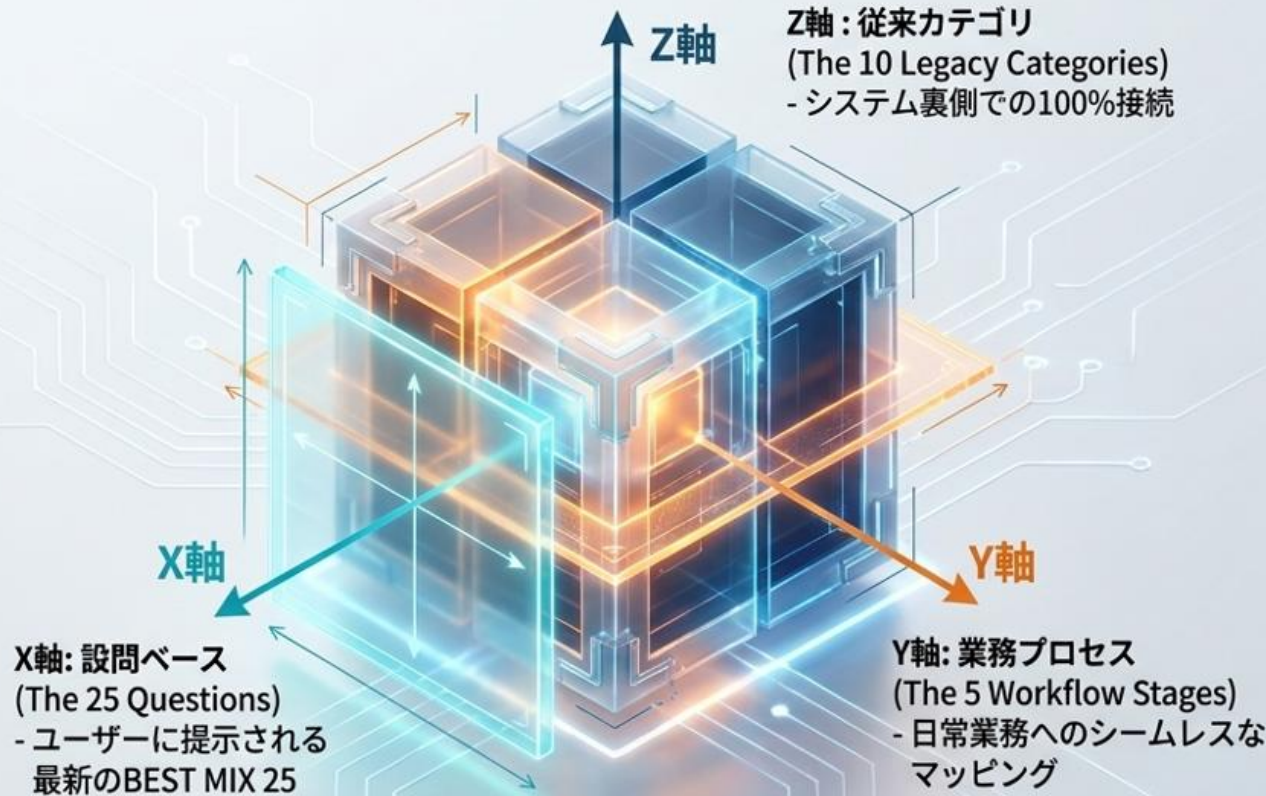
内部不正・ デバイス紛失

テレワーク・移動中における
物理的セキュリティと、
アクセス権限の過信

最新のAI脅威に目を奪われがちな今こそ、**足元の基幹リスク**に対する
意識の緩み（経年劣化）を正確に測定する必要がある。

※具体的な質問数は協議の上、決定します。

カテゴリ別の準ベンチマークを実現



革新的アーキテクチャの 戦略的価値

No Broken Benchmarks

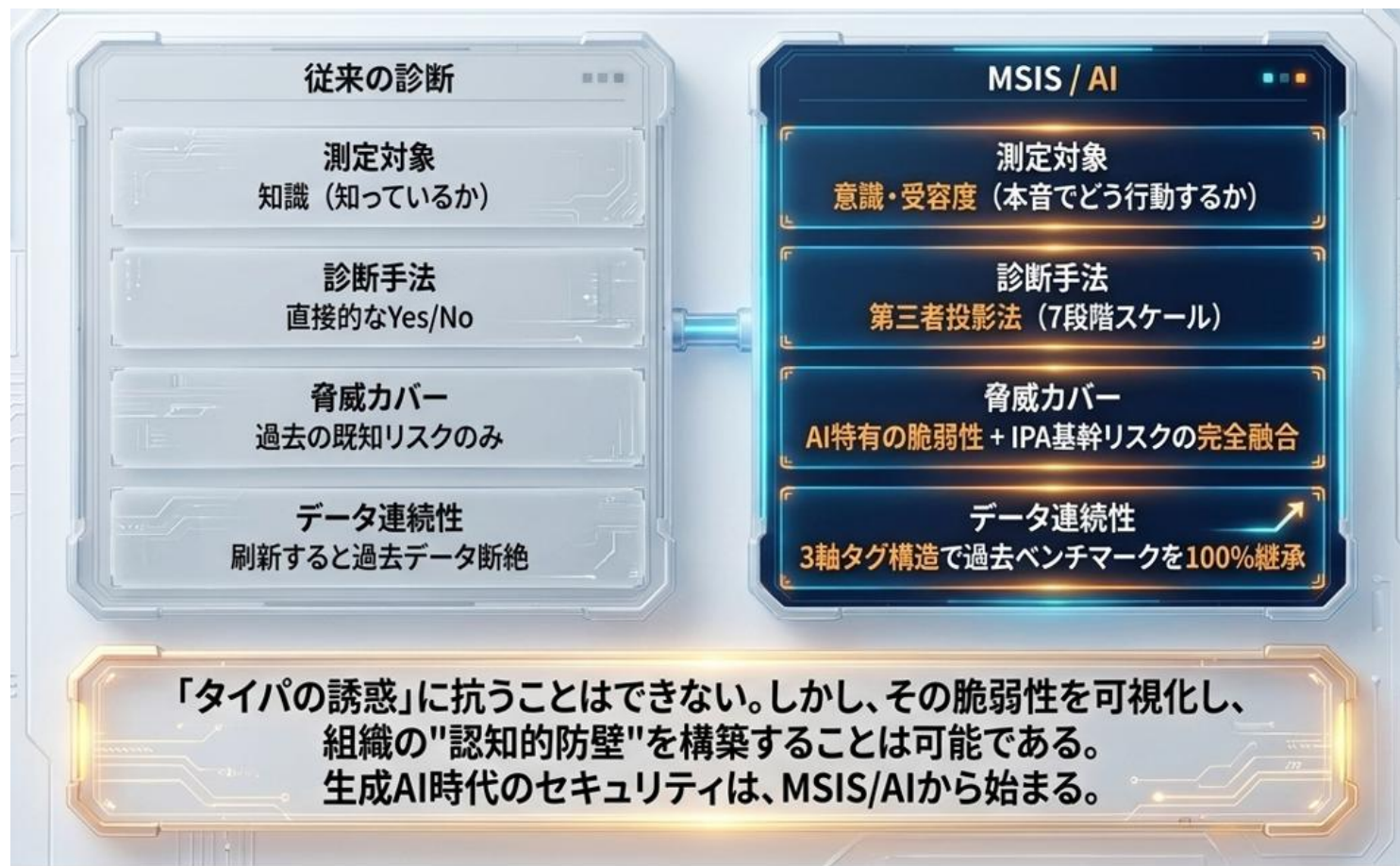
過去の経年変化データや、他社比較ベンチマークを一切損なうことなく、最新のAIリスク診断へ完全移行可能。

Invisible Upgrade

ユーザーには最新の25問を見せつつ、システム裏側では従来の10カテゴリと100%接続される。

※スクウェイブではこれまで10年以上のMSIS診断を実施しており、膨大なケースが蓄積されています。
※蓄積したデータとカテゴリ（約10個）の単位で比較分析を試みます。他組織のトレンド比較を実現します。

MSIS/AIで意識レベルの可視化を！



※ご連絡お待ちしております。
株式会社スクウェイブ
<https://www.k2wave.biz/contact>