生成AI利用ルールテンプレート
～ 安全なAI活用推進のために～

日本スマートフォンセキュリティ協会
セキュアAI活用推進タスクフォース
中村 丈洋

本日のトピック

JAPAN SMARTPHONE SECURITY ASSOCIATION

■セキュアAI活用推進タスクフォース の活動紹介

■成果物 - AI利用ルールテンプレート の解説

登壇者紹介

なかむら たけひろ
中村 丈洋

博士(工学)

JSSEC 利用部会

セキュアAI活用推進TF リーダー

【所属企業】

SHIFT SECURITY

「ソフトウェアテスト」で有名な

SHIFTグループに所属する

サイバーセキュリティ企業です

〔事業内容〕

脆弱性診断、セキュリティ監視、

インシデント対応支援、コンサルティング 等

サイバーセキュリティ全般に対応

JSSEC
セキュアAI活用推進タスクフォース
活動紹介

セキュアAI活用推進タスクフォース の活動

- 設立: 2025年7月（1年間の期限付き組織）
- 主な活動: 月次での定例会議
  - 方式: 現地＆リモートのハイブリッド
- その他
  - JAPAN SecuritySummit2025 で JSSECを代表して活動紹介
- タスクフォース メンバー: 5社 11名

KDDI 株式会社
上松 晴信
本間 輝彰

ソフトバンク株式会社
笠原 正弘

株式会社SHIFT SECURITY
小笠原 徳彦
中村 丈洋

株式会社ウィザース
岩波 一樹
重光 ちかこ

株式会社ラック
仲上 竜太
倉持 浩明
宮崎 力
野田 健

セキュアAI活用推進タスクフォース の目的

JAPAN SMARTPHONE SECURITY ASSOCIATION

目的

AI時代の変化に対応し、**AI活用の可能性をセキュア**に実現する

- **AI時代の変化**
  - **スマートデバイス**を介して**否応なく「AIが隣人」として存在**

- **AI時代の可能性とリスク**
  - 生成AIの活用自体は大きな可能性を持つ
  - 一方で**AIを受け入れる体制が不十分な社会**がリスクを生む

JSSECらしい「AI活用の可能性をセキュアに実現する方法」を模索
→「生成AI利用ルールテンプレート」の作成・公開 を企画

AI活用を阻害する大きな課題

JAPAN SMARTPHONE SECURITY ASSOCIATION

課題①　**AI利用リスクの把握・管理**が困難

↓ **リスク把握できない**から**ルール策定が困難**

↑ **ルールが無い**から**リスク管理が困難**

課題②　利用各社での「**AI利用ルール**整備」の遅れ

セキュリティ対策を組織的に行っていない ＝ 70%(※1)
中小企業が独自にルール整備することは困難

これらの課題解決には

「**利用者向けルール のテンプレート**」の**社会全体での普及**が有効

→ **専門知識無くてもルール策定**できる

→ **ルール策定を通してリスク把握・管理**ができる

※1 IPA: 2024 年度 中小企業における 情報セキュリティ対策に関する実態調査: https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1

既存のAI関連ガイドライン

「利用者向けルール のテンプレート」策定に先立ち、既存の活動を調査

■ 様々な団体がAI関連の文書・ガイドラインを公開

- JNSA: 生成AIを利用する上でのセキュリティ成熟度モデル
- JDLA: 生成AIの利用ガイドライン
- IPA: テキスト生成AIの導入・運用ガイドライン
- 経産省: AI事業者ガイドライン
- 経産省: AIの利用・開発に関する契約チェックリスト
- OWASP: OWASP Top10 for LLMs
- CSA: AI Controls Matrix

■ いずれも「利用者向けルール のテンプレート」ではない

→JSSECで「生成AIの利用者向けルール のテンプレート」整備を推進

目標とする利用ルールテンプレートの特徴

特徴①	組織の規模・状況に合わせて利用しやすい
特徴②	ルールの出所や根拠が明確
特徴③	利用者が理解しやすいルール

これらの特徴を持つ「テンプレート」を提供することで
「**すべての組織**」で「**AI利用ルールの策定**」を可能にします

特徴① 組織の規模・状況に合わせて利用しやすい

■ ルールのレベル分け

- ルール毎の必須・推奨、厳格さをレベリング

■ ルールの取捨選択

→「AI基盤の契約内容」や「組織の状況」に応じて取捨選択

- 例）AIの無償プラン ・・・ AIのモデル学習に入出力が利用される

→ 情報漏洩等の対策として「厳格なルールの選択」が必要

特徴② ルールの出所や根拠が明確

ユースケースからAI活用リスクを洗い出し

●AIの挙動や利用者の行動によるリスクの列挙

リスク例）誤情報の拡散、著作権の侵害、フィッシング、ファイル誤アップ・・・

●「情シスが用意したAI」の外にも脅威がある

情報漏洩の脅威例）個人スマホでの会話要約、ホワイトボードの文字起こし
新たな脅威例）AIと連携した眼鏡型デバイス等

外部ガイドラインから対応ルールを洗い出し

●外部ガイドライン: IPA や 経産省 等が公開

外部ガイドラインとの関係性を明示
ルールの網羅性を把握

特徴③ 利用者が理解しやすいルール

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ルールが意図するリスクを解説

→策定者: ルールの取捨選択・リスク管理の情報

→利用者:「なぜルールを守らないといけないか」を自覚

■ルールは少数・簡潔

長大・複雑なルールは実効性が無い

→　ルールは少数・簡潔に。具体例で説明

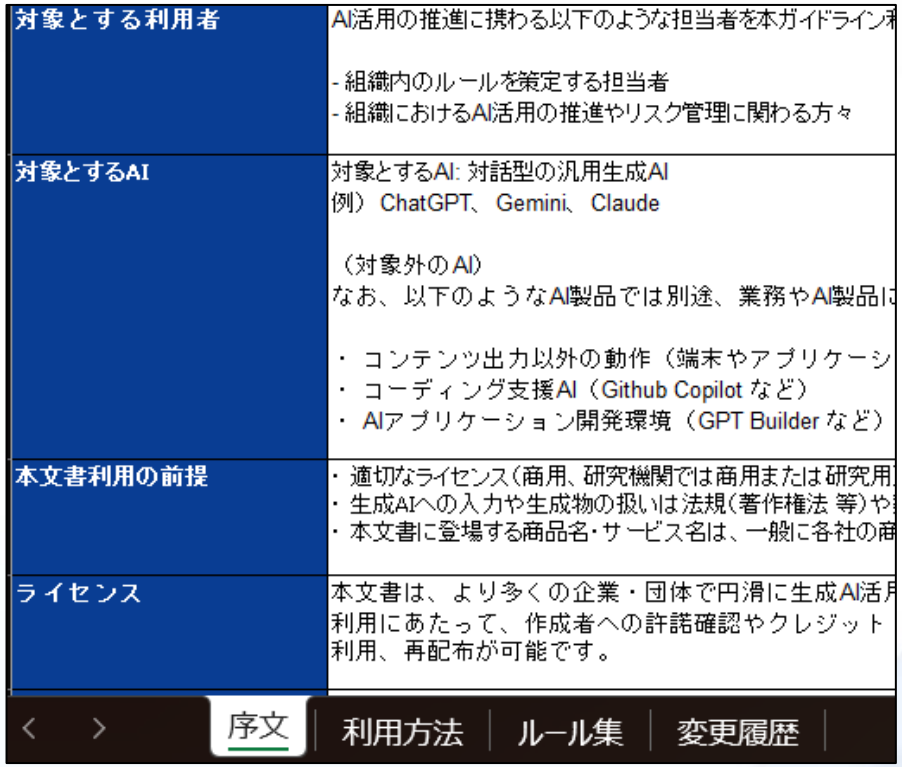
成果物 - AI利用ルールテンプレートの紹介

成果物-AI利用ルールテンプレートの構成

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ Excel形式で配布

- **序文**
  - 文書の目的、ライセンス、免責事項など
- **利用方法シート**
  - テンプレートを利用したルール整備の方法を解説
- **ルール集**
  - テンプレート本体
- **変更履歴**
  - 変更履歴と製作団体・製作者クレジット



基本的な使い方

■ 「ルール集」シートに**ルール記載事項**と**取捨選択の指針**を列挙

- 全18ルール、68の行動 から取捨選択

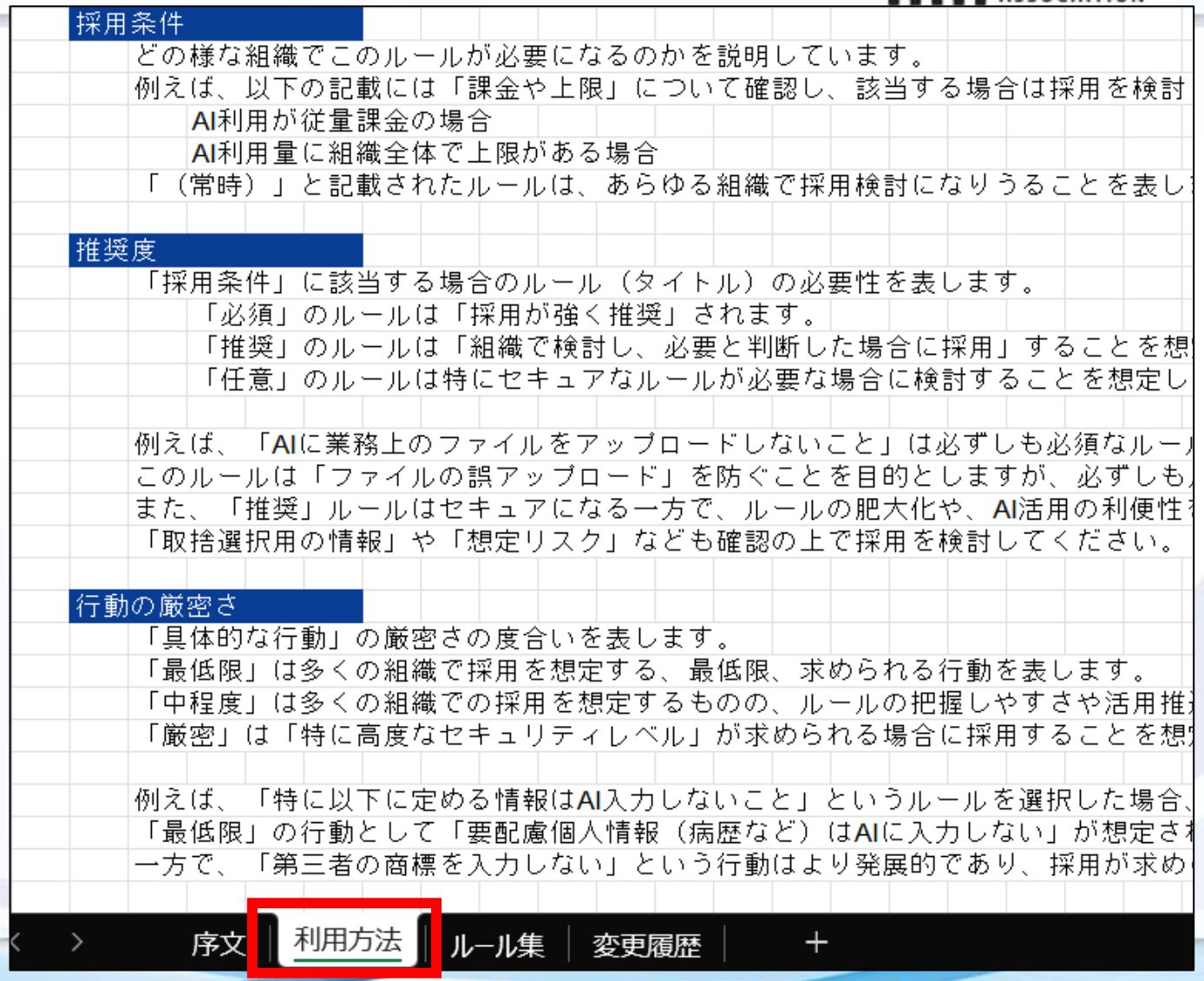
選択したルールを各社書式にコピペして利用

シーン	カテゴリ	採用条件	タイトル	推奨度	具体的な行動（取捨選択）	行動の厳密さ	取捨選択用の情報	想定リスク	選択	ルール選択メモ
AIを利用する前に	アクセス方法	（常時）	許可されたAIサービスのみを正しいIDで利用すること	必須	以下のURLをブラウザのブックマークに登録してアクセスする 【※組織毎に修正※】http://example.com/xxx	最低限		【フィッシング】 検索サイトやメールや外部サイトのリンク経由でアクセスした場合、見た目がそっくりな偽サイトに誘導される場合があります。		
					Web検索結果からアクセスしたAIサービスサイトへ情報を入力しない	中程度		偽サイトにID/パスワードや重要情報を入力すると情報漏洩になります。		
					指定されたIDでログインしていることを確認する	中程度				
					以下の専用クライアントアプリを常に利用する。 【※アプリ名を指定※】	厳密	PCやスマホの専用クライアントアプリからAIを利用する場合にはこちらを検討ください。 クライアントアプリでの利用を強制することで、ブラウザ上でのフィッシングリスクを低減できる場合があります。	【無償版を通した情報漏洩】 誤ってログインせずにAIサービスを利用したり、無料版のAIサービスを利用した場合、入出力が外部に漏洩するリスクが生じます。 これは無料版と有償版では情報の取り扱いポリシーが異なるためです。		
					許可されていないAIサービスを利用しない	最低限				
	利用上の制限	（常時）	生成AIのリスクを理解し、適切な用途で利用すること	推奨	生成AIは不適切な出力をする場合があることを理解して利用する			【サービス上の制限】 生成AIに限らず、サービスには様々な制限や注意事項があります。		
					利用規約を理解したうえで利用する	厳密	組織ルールとして必要な場合は選択ください。 「生成AIの利用規約の理解」は利用者各人に求められますが、利用ルールとして明文化することは必ずしも一般的ではありません。	特に一般的な生成AIは出力の確かさを保証できないため、それによって生じる問題の責任は利用者に帰される傾向があります。 また「入力した情報がAIサービス提供者でどの様に扱われるか」を把握することも安全な利活用では重要になります。このような情報を利用規		
					利用する生成AIのプライバシーポリシーを確認する	厳密	利用規約と同様です			
	外部連携	利用者がMCPやプラグインを導入できる場合	生成AIの連携機能はリスクを理解して利用すること	推奨	連携プラグイン/MCPの導入は社内ルールに従った許可を得ること	中程度	利用者がMCPやプラグインを導入できる場合に検討してください。 このAI利用ルールの対象者が MCP や プラグインを導入できない場合には、この項目は対象外です。 例）システム管理者のみが設定できる場合は対象外 MCPは生成AIと様々なリソース・システムを連携するための仕組です。 本ルールの対象となる生成AIが「MCPホスト」となり、「MCPクライアント」を登録することで組織内データ・ツールなどを持つ「MCPサーバ」と連携します。	【外部連携機能を通した情報漏洩】 AIシステムに外部サービスとの連携プラグインやMCP(生成AIと各種リソースを連携するための仕組)連携を設定できる場合、それらを通して情報が外部に送信される可能性があります。 外部プラグインやMCPを利用する場合、それにより、どのような情報が外部に送信されるかを把握し、適切な承認を得る必要があります。 正しく送信情報を把握しなかったり、適切な承認を得ない場合には、情報漏洩等のリスクが生じます。 【AIによる過剰な自律性】 AIに過剰な自律性を与えた場合、意図しない処理 や データの破壊 等が生じる場合があります。 特に社内リソースをAIで処理できるようなプラグイン/MCPを利用する際には正しく、影響を評価し、必要に応じて機能の制限や人間による判断フローを導入することが求められます。		
					外部サービスとの連携プラグイン/MCPは、入力データが第三者に送信されることを同意したうえで利用すること	最低限				
					社内リソースとの連携プラグイン/MCPは、リソースに対する影響を評価したうえで利用すること	最低限				

基本的な使い方

「利用方法」シートで
基本的な利用方法を解説

どの様に「ルールを取捨選択」
するかを**例示を交えて解説。**



項目紹介 – ルールへ転記する項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

シーン：ルールが必要になるシーン
シーン毎にルールを整理することで把握しやすく

具体的な行動：ルールで守るべき具体的行動
「具体的にどうしたら？」を列挙

シーン	タイトル	具体的な行動（取捨選択）	想定リスク
AIに入力する	不必要に機微な情報をAIに入力しないこと	業務上、必要のない機密情報はAIに入力しない	【法令違反のリスク】 業務や扱う情報によっては、「情報の移転先」や「扱ってよいシステムの要件」などが法令で定められている場合があります。 利用するAIサービスがこれらの要件を満たさない場合に該当する情報を入力すると法令違反のリスクを生じます。 また、AIで扱うこと自体に問題が無い場合でも、そのAI生成物の扱いが不適切な場合にも法令違反に成りうるため注意が必要です。
		要配慮個人情報（病歴など）はAIに入力しない	
		個人情報・顧客情報を入力しない	
		社外秘の情報など、業務上の秘密を入力しない	
		外部共有用の成果物を作成する際は、機密情報（個人情報など）を伏せ字にするか仮名化してから入力する	既存システム」と要件に差異が無いか、などを確認してください。 【モデル学習利用による情報漏洩】※モデル学習に利用されない
	第三者に権利があるデータを入力しないこと	第三者の著作物や商標を入力しない	【法的リスク】 入力が学習データとして利用される場合、第三者が権利を有するデータの入力は著作権や肖像権を侵害する法的リスクが生じます。 学習データとして利用されない場合でも、第三者が権利を有す

タイトル：ルールのタイトル
「注意すべきこと」を**端的に表現**

想定リスク：ルール違反で生じるリスク例
「なぜ守らなければならないか？」を理解

項目紹介 – ルールの取捨選択に利用する項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

採用条件：ルールが必要/不要な条件
例）AI利用が従量課金 → ルール「コストを意識して利用」

推奨度：ルールの必要性の目安
例）不必要に機微な情報をAIに入力しない → 必須
　　第三者に権利があるデータを入力しない → 任意

取捨選択用の情報：取捨選択のヒント
ルール策定者に向けたガイド

採用条件	タイトル	推奨度	具体的な行動（取捨選択）	行動の厳密さ	取捨選択用の情報
AI利用が従量課金の	コストを意識して利用すること	推奨	大容量データの入力や大量の問い合わせを行わな	厳密	従量課金であったり、1人が大量に利用すると、他の利用者が制限を受ける場合には、この
			単純な問い合わせにはコストの低いモデルを指定	中程度	
（常時）	不必要に機微な情報をAIに入力しないこと	必須	業務上、必要のない機密情報はAIに入力しない	最低限	以下の場合には検討ください。 ・法令やコンプライアンスで求められる ・入力がモデル学習に利用される
			要配慮個人情報（病歴など）はAIに入力しない	最低限	
			個人情報・顧客情報を入力しない	中程度	
			社外秘の情報など、業務上の秘密を入力しない	中程度	なお「当該情報の漏洩対策」自体は別項目（AIの出力を利用する>機微情報の保
			外部共有用の成果物を作成する際は、機密情報	中程度	
（常時） ※「学習有りの生成AI」の場合は必須	第三者に権利があるデータを入力しないこと	任意	第三者の著作物や商標を入力しない	最低限	「入力データが生成AIの学習に利用される場合」には必ず検討してください。 「出力を介した権利侵害のリスク」は別項目（AI
			第三者の顔写真やプロフィールを入力しない	最低限	
			権利を失うことを許容できる情報のみ入力すること	厳密	入力が学習データとして利用され、かつ、想定リスクの【権利の喪失】を許容できない場合に検討ください。

行動の厳密さ：「具体的な行動」の厳密さ
「厳密すぎる行動」は省くこともAI活用に重要

特徴）利活用とセキュリティのバランス

■ **シーン**:機微情報の入力

■ **ルール**: 不必要に機微な情報をAIに入力しないこと

■ **具体的な行動**

- （最低限）業務上、必要のない機密情報はAIに入力しない
- （中程度）外部共有用の成果物を作成する際は、
  機密情報を仮名化してから入力する
- （中程度）要配慮個人情報（病歴など）はAIに入力しない
- （厳密）個人情報・顧客情報を入力しない
- （厳密）社外秘の情報など、業務上の秘密を入力しない

AI利活用を阻害する厳密な制限は取捨選択可能に
※「漏洩対策」は別項目（出力>機微情報の保護）で対応
→ 各社にあった「利活用とセキュリティのバランス」を可能に

特徴）スマートデバイス関連のルール

スマートデバイスについて**3つのルール**を用意

■ ルール①: 業務中は**無許可の私用ウェアラブルデバイス**を利用しないこと
- 採用条件 ＝ 常時

■ ルール②:**許可された端末**を**ルールを守り利用**すること
- 採用条件 ＝ スマートフォンでのAI利用を許可する場合

■ ルール③:**私用スマートフォン**の**禁止事項を守る**こと
- 採用条件 ＝ 私用スマートフォン（BYOD）を利用する場合

スマートデバイス関連ルール – ウェアラブルデバイス

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ **ルール: 業務中は無許可の私用ウェアラブルデバイスを利用しないこと**

- 採用条件 ＝ 常時、推奨度 ＝ 必須

■ 具体的な行動

- （最低限）業務中は眼鏡型デバイスを停止すること
- （最低限）業務中は環境音をAIで分析する機能を停止すること
- （最低限）業務中はライフログ製品を停止すること
- （中程度）**業務上の理由（視覚・聴覚の補助等）でデバイスの使用が必要**な場合は**許可の下、定められた範囲で利用**すること

多様な人々が活躍する社会では**ウェアラブルデバイス**は身近な存在に
一律禁止では社会のニーズに対応できない
→ **組織の状況**に合わせて**必要な条項を選択可能**に

発展：外部ガイドラインとの対応

外部ガイドライン項目をルールに紐づけ

→「外部ガイドラインへの対応状況」を容易に把握可能

【不必要に機微な情報をAIに入力しないこと】に紐づく外部項目

【東京都デジタルサービス局】
ルール1: 個人情報等、機密性の高い情報は入力しないこと

【経産省：AI事業者ガイドライン】
U-4）i. 個人情報の不適切入力及びプライバシー侵害への対策
…個人情報を不適切に入力することがないよう注意を払う
U-5）i. セキュリティ対策の実施
…機密情報等を不適切に入力することがないよう注意を払う

【JDLA：生成AIの利用ガイドライン】
…以下の類型のデータを入力する場合、特に注意が必要です。
…
⑷ 個人情報
⑸ 他社から秘密保持義務を課されて開示された秘密情報
⑹ 自組織の機密情報

【IPA：テキスト生成AIの導入・運用ガイドライン】
以下に示す情報は、ユーザによる入力を制限することが推奨されます。
…
・ 個人情報
・ 組織の機密情報

普及促進のためのライセンス選定

■ **CC0**;クリエイティブ・コモンズ・ゼロ での公開を検討

CC0 = パブリックドメイン として、**誰でも自由に改変・再配布**できる

【なぜ CC0？】「各社ルールのテンプレート」に最適

「自社ルール」に「JSSEC の クレジット表記」を強制しないため

→ 利用組織の**法務（ライセンス）チェックを低減**
→ **活用を促進**する

「JSSEC の クレジット表記」を求める**「CC BY（表示）」と比較検討**し
テンプレートに**最適なライセンスを模索**した

課題 – ルールの対象範囲

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ **対象は「対話型の汎用生成AI」**

- 対象の例）ChatGPT、Gemini、Claude 等

■ **以下への対応は不十分**

- コンテンツ出力以外の動作をする**AIエージェント**
- **コーディング支援AI**
- **AIアプリケーション開発環境**

特に**近年は「AIエージェント」が普及**しつつある

AIエージェントへの対応は今後の課題

謝辞

タスクフォースに参加頂いた皆様（5社11名）

KDDI 株式会社
上松 晴信
本間 輝彰

ソフトバンク株式会社
笠原 正弘

株式会社SHIFT SECURITY
小笠原 徳彦
中村 丈洋

株式会社ウィザース
岩波 一樹
重光 ちかこ

株式会社ラック
仲上 竜太
倉持 浩明
宮崎 力
野田 健

ご協力ありがとうございました！

今後の活動予定

■ JSSEC内レビュー
- 予定: 2月中旬 ～ 3月中旬

■ 一般公開
- 予定: 3月末

■ 来期以降の活動について
- 当タスクフォースは1年間の期限付き活動です。
- 皆さまからの ご意見が次年度の活動につながります
  - 成果物活用のワークショップなども検討しています
  - ぜひ、皆さんのご意見・ご参加をよろしくお願いします！

JAPAN SMARTPHONE SECURITY ASSOCIATION

ご清聴ありがとうございました

予備スライド

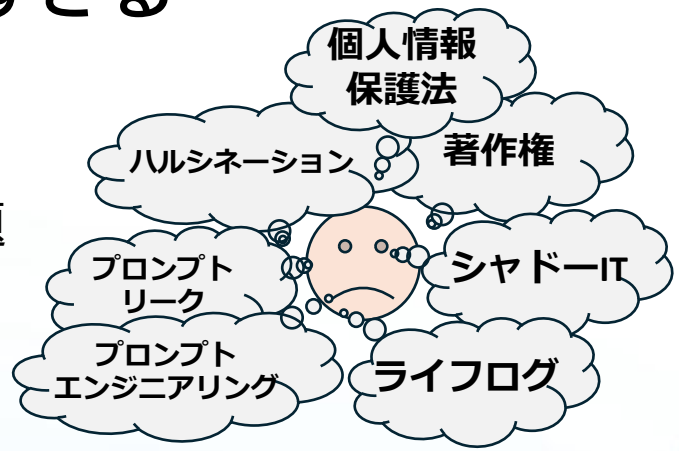
課題① 利用各社におけるAI利用リスクの管理困難

JAPAN SMARTPHONE SECURITY ASSOCIATION

AIを利用したくても「AI利用リスク」の把握・管理が困難

■ ルール策定者・利用者 に「AI特有の問題」を求めすぎる

- 例）著作権 や ハルシネーション（幻覚）・・・
- 一方で「ルール策定・遵守に**不要な情報**」も氾濫
  - 例）プロンプトリーク → AIを利用したシステム構築で注意すべき問題



■ 広範囲のリスク分析が必要

- 例）コンプライアンス上のリスク、法令リスク、情報漏洩リスク・・・
- **「正しい使い方」**だけでは問題をカバーできない
  - 「AI製品のシャドーIT化」など「正しくない使い方」の分析も重要

    身近なAI製品の例）スマホの要約・翻訳機能、ライフログ製品など

課題② AI活用ルール整備の遅れ

JAPAN SMARTPHONE SECURITY ASSOCIATION

AIを利用したくても「社内ルールの整備」が追い付かない

■「各社に合わせたAI活用ルール」が必要

- **各社の状況・ポリシーに合わせたルール**が必要（契約形態、業種、扱う情報など）
- 「あるべき」の**厳しすぎるルール**はAI活用を阻害するだけでなく、**シャドーITの温床**に・・・

■ 一方、実情では「独力でのAI活用ルール策定」は困難が大きい

- 中小企業での情報セキュリティ対策の状況

  組織的に行っていない ＝ 70%（兼務/専門担当者がある ＝ 30%）

  中小企業が独自にルール整備することは困難が想定される
  「AI固有リスクを独自に調査」し「自社に合わせたAI活用ルール」を策定する・・・中小企業以外でも容易ではない

IPA: 2024 年度 中小企業における 情報セキュリティ対策に関する実態調査
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

項目紹介 – ルールへ転記する項目

■ **シーン**: ルールが必要になるシーン
- **シーン毎にルールを整理**することで把握しやすくする
- 例）AIを利用する前に、AIに入力する

■ **タイトル**: ルールのタイトル
- **「注意すべきこと」を端的に表現**する
- 例）不必要に機微な情報をAIに入力しないこと

■ **具体的な行動**: ルールで守るべき具体的な行動
- 端的なルールでは把握しずらい**「具体的にどうしたら？」**を列挙
- 例）業務上、必要のない機密情報はAIに入力しない
- 例）個人情報・顧客情報を入力しない

■ **想定リスク**: ルール違反で生じるリスク例

項目紹介 – ルールへ転記する項目

■ **想定リスク**: ルール違反で生じるリスク例

「不必要に機微な情報をAIに入力しないこと」のリスク（抜粋）

【法令違反のリスク】

業務や扱う情報によっては、「情報の移転先」や「扱ってよいシステムの要件」などが法令で定められている場合があります。

利用するAIサービスがこれらの要件を満たさない場合に該当する情報を入力すると法令違反のリスクを生じます。

また、AIで扱うこと自体に問題が無い場合でも、そのAI生成物の扱いが不適切な場合にも法令違反に成りうるため注意が必要です。

代表的な法令としては 個人情報保護法 等が上げられます。

AI利用時には法令の定める要件を満たすか、また「要件を満たす既存システム」と要件に差異が無いか、などを確認してください。

【モデル学習利用による情報漏洩】※モデル学習に利用されない（有料プランなど）場合は除外できます

AIサービスやプランによっては入力データがモデルの改善に利用されます。

このような場合、AIサービス提供者がデータを閲覧したり、学習データを通して、入力データが第三者に開示される場合があります。

このため、入力データがモデル改善に利用される場合に 個人情報、顧客情報、営業秘密 等を入力すると情報漏洩になります。

・・・

項目紹介 – ルールの取捨選択に利用する項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ **採用条件**: ルールが必要/不要となる条件

- 例）AI利用が従量課金の場合、組織全体で上限がある場合
  → ルール：コストを意識して利用すること

■ **ルールの推奨度**: 採用条件に合致する場合のルールの必要性の目安

- 必須: 不必要に機微な情報をAIに入力しないこと
- 任意: 第三者に権利があるデータを入力しないこと

■ **行動の厳密さ**: 「具体的な行動」の厳密さ

- 最低限: 第三者の著作物や商標を入力しない
- 厳密　: 権利を失うことを許容できる情報のみ入力すること

■ **取捨選択用の情報**: 取捨選択のヒント

- 入力が学習データとして利用され、かつ、想定リスクの【権利の喪失】を許容できない場合に検討ください。