概要

企業戦略に基づくセキュリティ戦術の策定
-生成AIとセキュリティガイドラインの考察-

■想定読者

企業セキュリティの企画責任者、担当者(特に、企業セキュリティを推進する責任者、担当者)

■背景・課題

近年のサイバー攻撃の高度化・多様化や企業のデジタル化の推進に伴い、企業においてセキュリティ戦略・戦術を策定する必要性が増している。その一方で、必ずしも戦略・戦術の策定は順調ではないと考えている。

・戦略、戦術の全体像が分からない。
・参考になるはずのガイドラインの正しい使い方が分からない。
・生成AIの有用性、活用例、注意点が分からない。
・作成したセキュリティ戦略・戦術の見直しがなされない。

■考察

セキュリティ戦略と経営戦略
・企業におけるセキュリティ戦略は**経営戦略等**から導き出されるべきである。
・セキュリティ戦略の実現は**経営戦略の実現**に寄与するべきである。

セキュリティガイドラインの活用
・セキュリティガイドラインは**前提となる思想**を理解した上で利用を行うべきである。
・セキュリティガイドラインは自社の状況に応じて**カスタマイズ**を行うべきである。

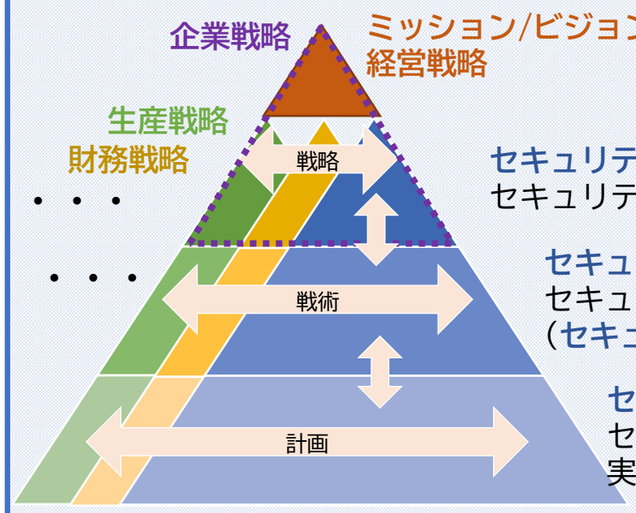
生成AIによるセキュリティ戦術の策定
・企業セキュリティの企画責任者、担当者はセキュリティ戦術の**妥当性を評価できる戦略的思考**が求められる。

■セキュリティ戦略と経営戦略

企業戦略において、最上位にあたるミッション、経営戦略等が存在する。この経営戦略から、生産戦略、財務戦略等、様々**機能別戦略が導き出されるとともに、経営戦略の実現**に寄与しなければならない。

機能別戦略の1要素として、**セキュリティ戦略**が存在するとともに、**セキュリティ戦術、セキュリティ計画**が存在する。

セキュリティ戦略/戦術/計画は他の戦略/戦術/計画と相互に連携する場合もあり、更に包含関係、上下関係等の複雑な関係がある。



■セキュリティガイドラインの活用

セキュリティガイドラインは、セキュリティ戦術(What:何を行うか)の検討にあたり、指針となるものである。セキュリティガイドラインには信頼性、柔軟性、効率性のメリットがあり、下記特徴があることを発見できた。

考察理由：

サイバーセキュリティは、業種、環境、システム構成に応じたリスクが存在する。

セキュリティガイドラインの**前提となる思想**（例:IEC62443におけるPurdue model）を理解することで、**自社にとって最適なガイドラインを選択**することが出来る。

更に、自社のビジネスリスクに応じて**ガイドラインの内容を取捨選択、読み替え**をすることで、自社にとって最適なセキュリティ戦術の策定が可能となる。

■生成AIによるセキュリティ戦術の策定

今回のユースケースにおいて、生成AIは経営戦略等からセキュリティ戦略、セキュリティ戦略からセキュリティ戦術の作成において、即座にドラフトを作成・自身とは異なる視点のアイデアを創出できることを確認できた。

考察理由：

生成AIは仕組み上、入力されたデータを元に**妥当と考えられる文章を作成**するシステムである。そのため作成したセキュリティ戦術の妥当性評価を行える人材の価値が高まると考えた。

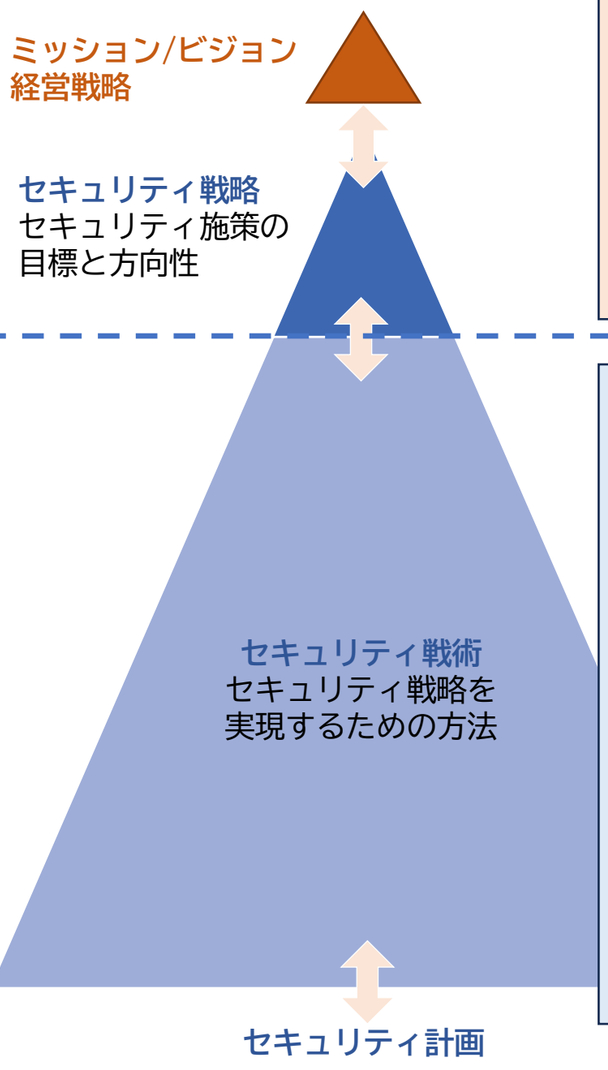
生成AIを用いた
セキュリティ戦術作成例

企業戦略に基づくセキュリティ戦術の策定
-生成AIとセキュリティガイドラインの考察-

本プロジェクトでは実企業の経営戦略から生成AIを用いてセキュリティ戦術を作成した。その作成プロセスとプロンプト例を**活用例**として示す。生成AIを用いることで、経営戦略（中期計画、グループレポート等）からセキュリティ戦略・戦術への落とし込み、評価・改善の役割を担わせる。そして、現状の生成AIにセキュリティ戦術を実現することは、物理的、技術的に困難、かつ責任が取れないものである。そのため、実現可能性や妥当性の最終判断は、 “人”が行わなければならない。

注意点：
- 生成AIを実業務で利用する場合は、自社のルールに従うこと
- 各STEPにおいてプロンプト出力がインプット情報に基づく内容となっているか、都度確認を行うこと
- 各STEPにおいて意図しない出力となった場合は、都度修正や、再入出力を行うこと

■セキュリティ戦略と経営戦略



※ピラミッドの大きさは情報量、重要性を示していない事に注意

■生成AIの活用

1．セキュリティ戦略作成

	生成AI　プロンプト例
STEP1：経営戦略からセキュリティ戦略作成	（アップロードした中期計画等の）資料から経営戦略を抽出してください。 また、抽出した経営戦略よりセキュリティ戦略を作成してください。

※セキュリティ戦略がすでに存在する場合は、STEP2から実行する。

セキュリティ戦略が存在しない場合は、中期経営計画やミッション、経営戦略等からセキュリティ戦略を作成する。

2．セキュリティ戦術作成・改善

	生成AI　プロンプト例
STEP2：戦術の作成	出力したセキュリティ戦略を実現するためのセキュリティ戦術を作成してください。
STEP3:戦術の評価	評価指標(※)に基づき整合性、適合性、具体性の観点で、1～４段階で監査人の目線で評価してください。
STEP4：戦術の確認と改善	出力したセキュリティ戦術が高評価になるように戦術を再作成してください。

3．セキュリティ戦術の妥当性判断

	生成AI　プロンプト例
STEP5：セキュリティガイドラインの参照	出力したセキュリティ戦術に関連するセキュリティガイドラインを紐づけてください。
STEP6：戦術の妥当性を判断	**生成AIは用いない。 人が判断する。**

(※)STEP3における、評価指標は次の通り
整合性：経営戦略と論理的に結びついているか
適合性：セキュリティガイドラインと適合しているか
具体性：手順に展開可能なレベルで書かれているか