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

独立行政法人　情報処理推進機構産業サイバーセキュリティセンター
中核人材育成プログラム 8 期生　セキュリティガイドライン利活用推進プロジェクト

2025 年 8 月 29 日

目次

1. 概要

1.1. はじめに

近年、業務のクラウド化、IoT の活用、リモートワークの定着といった要因により、企業活動はデジタル環境への依存度を急速に高めている。このような環境の変化に伴い、サイバー攻撃も高度化・多様化しており、従来の境界型防御では対応が困難な状況が広がっている。

このような背景のもと、サイバーセキュリティはもはや IT 部門に閉じた技術的課題ではなく、事業の継続性と信頼性に直結する経営課題として、経営層においても重要性が認識されつつある。たとえば、内閣サイバーセキュリティセンターの『サイバーセキュリティ戦略』（2021 年）[1]や、経済産業省『DX レポート 2』（2020 年）[2]においても、経営層の関与や全社的なセキュリティ推進の必要性が繰り返し強調されている。

しかしながら、現場の担当者の間ではセキュリティ戦略やセキュリティ戦術を策定するにあたり、「何から着手すべきか分からない」「戦略や戦術といった言葉が抽象的すぎて捉えにくい」といった声が多く、そこから実行可能な施策として落とし込むことに苦慮しているのが実情である。

これに対し、NIST CSF や ISO 27001、CIS Controls 等、様々な機関から各種セキュリティガイドラインが公開されている。これらのガイドラインには、一定のセキュリティ水準を担保するための要素が整理されており、独自に施策を構築するよりも、迅速かつ網羅的にセキュリティ戦術を策定できるメリットがある。しかし、たくさんあるセキュリティガイドラインの中から何を選ぶべきか、どのように適用していくのかといった点については多くの企業が正しく理解しないまま、上司からの指示や同業他社が適用しているガイドラインに沿って適用を進めてしまうこともあるのではないかと感じている。そのため担当者としては、専門知識のみの習得やガイドラインを読み解くために膨大な時間と労力を要してきた。

そこで、近年注目を集めている生成 AI 技術を活用することで、これまで人手で行っていたガイドライン要素を取り入れたセキュリティ戦術策定を行えないかを検証し、その上で改めてセキュリティ戦術策定するために必要なことは何かを整理する。

本書では、まずセキュリティ戦術を策定する上で必要となる情報について考察し（2 章）、続いてガイドラインの課題・活用方法（3 章）、生成 AI によるセキュリティ戦術策定について考察する（4 章）。最後に、活用上の留意点と今後の展望を提示する（5 章）。

著者らは、日々のセキュリティ戦術策定やインフラ運用に携わる中で、ガイドラインや生成 AI の活用に課題を感じてきた。本書が同様の課題を抱える読者にとって、より実践的かつ効果的な戦術策定の一助となることを願う。

1.2. 目的

本書の目的は以下とする。

本書の目的：
企業戦略に基づく実効性あるセキュリティ戦術策定への提言

方針：
・セキュリティ戦術策定における関係情報の整理
・セキュリティガイドライン利活用における課題と注意点を整理
・生成 AI によるセキュリティ戦術の策定と課題の整理

1.3. 想定読者

企業セキュリティ戦略・戦術の関係者

1.4. 免責事項

- 本書の内容は、予告なく変更される場合がある。
- 本書の内容の正確性、完全性、最新性について、いかなる保証も行うものではない。
- 明示的または黙示的な保証（商品性、特定目的への適合性、第三者の権利を侵害しないこと等を含む）は一切行わない。
- 本書に記載された内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの公式な見解を示すものではなく、執筆者の見解に基づいている。
- 本書の利用、または利用できないことによって生じたいかなる損害・損失について、執筆者は一切の責任を負わない。
- 特に生成 AI の活用については、情報漏洩の可能性もあるため、必ず自社ルール、指示に従うこと。
- 本書の有効期限は、発行日より 2 年間とする。

2.　セキュリティ戦術策定に関わる戦略、戦術の関係性

セキュリティ戦略・戦術を策定することを考えた時に、そもそも何から導き出されるのか、戦略、戦術の全体像が分からない、という課題がある。これは企業において、ミッション、ビジョン、経営戦略、生産戦略、財務戦略・・・と様々な戦略が存在する中で、セキュリティ戦略やセキュリティ戦術がどの位置に該当し、それらはどのように関係するのかが明確でないことが原因と考えた。そのため、セキュリティ戦略・戦術策定に関連すると思われる情報についてその定義を見つめなおし、その関係性を考える。

2.1.　経営戦略

経営戦略とは、企業が長期的な視点に立ち、持続的な競争優位性を確立し、経営目標を達成するための方針、計画についてステークホルダ(株主、投資家のみならず、従業員、顧客等)に対して示すものである。

一例として、経営戦略から導き出される戦略として、個々の事業部門が、それぞれの市場においてどのように競争優位性を確立し、目標を達成するかを決定する事業戦略、各機能部門（生産、財務、人事、IT など）が、全社戦略や事業戦略の目標達成に貢献するための具体的な機能別戦略が存在する。これら戦略を総称して企業戦略と呼称する。

ここで大企業や上場企業の場合、経営戦略や Group Report といった「企業における将来像」を、IR 資料やホームページで明文化し公開している。一方で、中小企業の場合、企業理念や売上目標はあっても経営戦略を明文化されていないことも多く、約 3 割の中小企業が経営戦略を策定していない。[3]このような場合は経営者との対話を通じて自社の経営戦略を明確にする必要がある。

2.2.　DX 戦略

DX とは企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立することである。 [4]。

2.3.　セキュリティ戦略

セキュリティ戦略とは、経営戦略、DX 戦略を実現するにあたり、企業における資産を、様々な脅威から　保護等をするための包括的な方向性を示したものである。これは、事業継続性の確保、顧客からの信頼維持、法令順守といった観点から、企業活動を支えるうえで不可欠な要素である。例えば、セキュリティ侵害が発生した場合、直接的な財務損失に加えて、企業の評判低下や事業活動の停止といった深刻な事態を招き、結果として経営目標の達成を大きく妨げる可能性がある。反対に、強固なセキュリティ体制を構築する

ことは、顧客やビジネスパートナーからの信頼を得ることに繋がり、新たなビジネスチャンスの創出にも寄与するものである。

2.4. セキュリティ戦術

セキュリティ戦術とは、セキュリティ戦略で示された包括的な方向性を踏まえ、どのようにするべきかを定義したものとなる。一般に、ベースラインアプローチ、リスクベースアプローチといった方法が存在する。

- ベースラインアプローチ：あらかじめ定められた標準的なセキュリティ対策の基準（ベースライン）を設定し、その基準を満たしているかどうかを評価するアプローチであり、多くのガイドラインや業界標準、法律・規制などがベースラインとして用いられる。
- リスクベースアプローチ：組織にとって最も重要な情報資産を特定し、それに対する潜在的な脅威や脆弱性を評価、その上で、リスクの発生可能性と影響度を分析し、リスクの大きさに応じて対策の優先順位を決定する。

セキュリティ戦術を策定する際には、どちらか一方ではなく、組み合わせアプローチとして併用されることが多く、これにより効率性と効果性を両立させることが可能となる。

2.5. セキュリティ戦略、セキュリティ戦術の違い

戦略、戦術、計画は達成する目標達成を指す点で共通するが、その範囲、時間軸、具体性のレベルにおいて差異が見られるものである。

- セキュリティ戦略：抽象度が高く、長期的な視点で組織のセキュリティに関する基本的な方針、目標、原則を定めた上位概念であり、組織全体として何を達成したいのか、どのような価値を守りたいのかといった、「何をすべきかの方向性」(Why)を示すものである。
- セキュリティ戦術：セキュリティ戦略を実現するための要件であり、「どのようにすべきか」(How)を示し、組織全体で一貫したセキュリティレベルを維持するために用いられる。
- セキュリティ計画：セキュリティ戦術をより具体化した施策に該当する。セキュリティ戦術に定められた要件を実際に実行するための具体的なステップ、方法を記述したものである。「具体的に何を」(What)を示し、セキュリティ実装計画や、日々の運用における具体的な作業レベルまで落とし込んだものとなる。

本資料では、これらの定義を踏まえ、セキュリティ戦略は、組織のセキュリティに関する長期的な目標と、その目標を達成するための方向性の基本的なアプローチを定めるものとなる。戦略策定においては、組織のビジネス目標、リスク許容度、適用される法規制の

遵守などが総合的に考慮されるものとなる。セキュリティ戦略は、組織が、「なぜ」それを行うのかという指針を示すものとなり、長期的な視点から組織が目指すセキュリティの状態や、その実現に向けた基本的な方針を示すものとなる。

一方、セキュリティ戦術は、セキュリティ戦略で定められた目標を達成するために、具体的な行動計画に落とし込むための手段となる。

実業務においては、セキュリティ戦術はより具体的なレベルとなる計画に落とし込める要件を網羅する必要がある。ここで計画には具体的なセキュリティ対策の選択、導入、運用、監視といった、より詳細な活動が含まれ、これはセキュリティ戦術から導き出されなければならない。

具体的な例として、セキュリティ戦略において「従業員の教育プログラムの実施」という長期的な目標を掲げたとする。この目標を達成するための戦術としては、「セキュリティリスクを念頭に置きながら一般的な業務を遂行するための知識とスキルを習得できるよう、意識向上とトレーニングの実施」、及び、「専門的な役割を担う個人は、セキュリティリスクを念頭に置きながら関連する業務を遂行するための知識とスキルを習得できるよう、意識向上とトレーニングを実施」と考えられる。計画としては、「年 1 回以上の従業員共通教育の実施とフォロー」、「年 1 回以上の管理職員専用教育の実施とフォロー」となる。

上記のように、具体的な目標とそれを達成するための行動を明確に結びつけることで、戦略は実行可能で現実的な戦術となり、組織全体のセキュリティレベルの向上に直接的に貢献することが可能となる。

戦略を達成するためには、抽象的な目標を具体的な計画に落とし込む必要がある。戦術は、この橋渡しをする役割を担い、戦略目標の実現に向けた具体的な道筋を示すものとなる。

セキュリティ戦略と戦術は、それぞれ異なる役割を果たしながらも、組織のセキュリティ体制を構築・運用していく上で、不可欠な要素である。両者が緊密に連携して機能、一貫性と整合性が保たれることは、効果的なセキュリティ体制の構築、維持に対して極めて重要となる。

2.6. 経営戦略、及びセキュリティ戦略の関係性

企業において、経営戦略からセキュリティ戦略を含む様々な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ものである。

さらに機能別戦略は、相互に連携するとともに、包含関係、上下関係等の複雑な関係生の上で成り立っている。セキュリティ戦略、戦術、計画についても同様に、相互連携の上で成り立つものである。

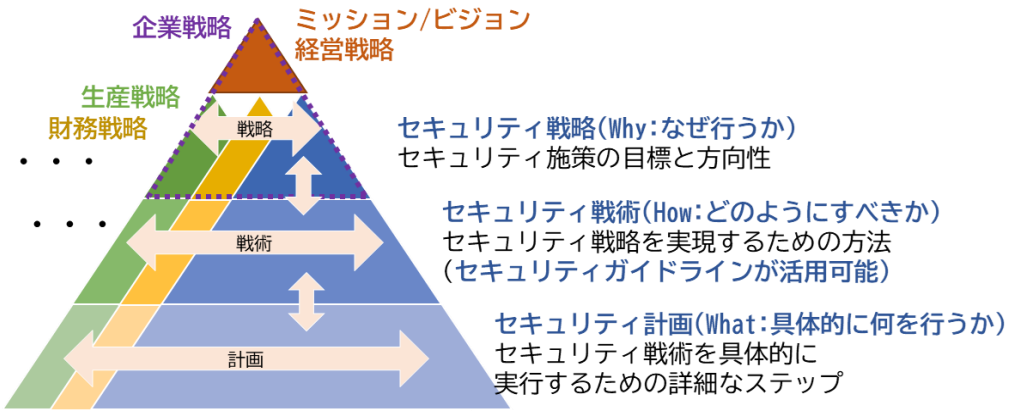

図１　経営戦略と各機能別戦略の関係性

しかし、効果的な戦術は単に戦略を一方的に落とし込むだけでは生まれず、現場の運用から得られる知見や課題認識を戦略や戦術にフィードバックするボトムアップの視点も重要である。さらに、戦術は企業リソース、コンプライアンス等を十分に考慮して策定され、外部環境の変化や新たな脅威に応じて柔軟に計画を変更する準備も必要である。

このように、経営戦略とセキュリティ戦略は相互に影響し合い、変化の速いビジネス環境において、両者が密接に連携し、現場の実情を踏まえた柔軟な戦略・戦術を展開していくことが、企業の持続的な成長と競争力強化の鍵となる。

3.　セキュリティガイドラインのセキュリティ戦術策定への活用

セキュリティガイドラインは、経営戦略およびセキュリティ戦略を踏まえたうえで、それらを具体的なセキュリティ戦術に落とし込むための枠組みとして活用されるものである。これは単なる技術的チェックリストではなく、戦略的意図を具体化するための行動指針として機能する。

とりわけ、セキュリティガイドラインは以下の観点において重要な役割を果たす。

- **共通言語化による意思疎通の促進と信用獲得**

セキュリティに関する用語や考え方を標準化することで、経営層や関係部署に加え、監査人・顧客・ベンダーといった社外関係者との間でも共通理解を醸成することで、円滑な意思疎通が図れる。さらに認知度が高いセキュリティガイドラインの活用は、対外的な信用獲得にも繋がるものである。

- **脅威と複雑性への対応**

サイバー脅威は高度化・巧妙化を続けており、システム環境も日々複雑性を増している。こうした変化に対応するため、セキュリティガイドラインは継続的に更新されており、組織はそれを参照することで最新の脅威に対応が可能になる。

3.1.　セキュリティガイドラインの課題

セキュリティ戦術策定にあたり、現在多種多様なセキュリティガイドラインが存在する中で、これらがセキュリティ戦略、戦術の策定に寄与することは認識していてもどのガイドラインを使うべきか分からない、または誤った使い方をした結果、建前だけのセキュリティ戦術になることで、セキュリティ強化につながらない、不十分な運用になってしまう可能性があると考えている。特に監査対応を目的として形式的にガイドラインを取り入れているものの、それが実際のセキュリティ強化には繋がっていないケースが見受けられる。

一般的にセキュリティガイドラインは抽象度が高く、そのまま適用する事は困難である。例えば、セキュリティガイドラインに「適切なアクセス制御の実装」と記載されていても、実際の業務システムにおいて「誰に」「どの情報への」「どのような操作権限を」「どのような運用ルールで与えるか」といった具体的な設計に落とし込むことが困難である。実務においては、営業部門、開発部門、経理部門で必要なアクセス権限は異なり、役職や担当業務によっても細分化される必要がある。ガイドラインの抽象的な記述だけでは、これらの詳細な権限設計の方針が定まらず、結果として過剰な権限付与や権限不足が発生する可能性がある。

また、一度作成した戦略・戦術が見直しされず、ビジネス環境の変化やガイドラインが更新されているにも関わらず、企業のセキュリティ戦略・戦術が古いままという状況が発生する。

また、2章で説明した通り、策定したセキュリティ戦略・戦術が経営課題と紐づかない、もしくは紐づけが弱いために不十分な可能性がある。経営戦略に「顧客情報の安全性の確保」と記載されていたとしても、それがセキュリティガイドラインのどの項目に当てはまるのかを正しく把握できず、結果として不十分なセキュリティ対策や、経営戦略との乖離が発生する可能性がある。

3.2. 選定について

ここまでで述べた通り、セキュリティ戦略を実現するための手段としてセキュリティガイドラインは有用である一方で、世の中には多種多様なセキュリティガイドラインがあり、のガイドラインを自社に適用すべきかを判断するには専門知識のみならず、膨大な時間と労力を要する。そのため、自組織にとって有用なセキュリティガイドラインを選定する必要がある時に次に挙げる2つの観点を考慮することが重要である。

3.2.1. セキュリティ戦略とガイドラインの関連性

セキュリティガイドラインを選定する際は、セキュリティ戦略の各要素に即して、その領域やテーマに最適化されたガイドラインを導き出すことが必要である。

3.2.2. 業種・業界・業態[1]の特性

業種・業界・業態によっては企業のセキュリティ戦術のために「活用すべきガイドライン」が存在する場合がある。これは、製造業における IEC62443 シリーズや、金融業における FISC 安全対策基準など法令や業界標準への対応、顧客・取引先との信頼関係構築のために、必要な要件となっているケースも存在する。

このように、各業界や業種にはその特性やリスク構造に即したがガイドラインが存在しており、たとえ企業戦略やセキュリティ戦略に明記されていなくとも、それを活用することが業界での信頼確保や事業継続を行うために必要である。

3.3. ガイドライン選定・利用の注意事項

ガイドラインを選定する際は、そのガイドラインが前提とするシステム構成が明示的、あるいは暗黙的に存在することに注意しなければならない。[2]そのため、自組織のシステム構成に照らし合わせて、効果を発揮するかを考える必要がある。

また、ガイドラインを利用する際は、基本的に自社に則した内容に変更、取捨選択するものである。そのため、ガイドラインを遵守すること自体を目的とするのは本来の使い方に反することに注意が必要である。(ISMS 等の認証取得の場合は、認証要件に関わるため、取捨選択はしてはいけない。)

---

[1] 業種・業界・業態の使い分けについては、業種は事業の種類(製造業など)、業界は経済活動の分野（自動車業界、製薬業界など）、業態は事業の形態(EC サイト、クラウドサービス提供など)を指すと考え、それぞれにセキュリティガイドラインが存在することを考慮し併記している。

[2] 一例として IEC62443 は Purdue Model による階層構造を前提としている。また明記はされていないものの、NIST SP800-53 は SC-7「BOUNDARY PROTECTION」の様に一般的な IT ネットワークの多層防御モデルを前提としている。

ガイドライン選定の具体例

ガイドライン選定における悪いケースとして、ガイドライン選定理由が「戦略との乖離」、「他社依存」の 2 つの例を示す。

例 1：戦略との乖離

悪いケース：

経営戦略からセキュリティ戦略を導き出すことが出来ない中で、ひとまず、戦術レベルのことが書いてあるガイドラインである NIST CSF2.0 を選定し出来そうなところから戦術を策定した。

良いケース：

経営戦略からセキュリティ戦略を導き、セキュリティ戦術を考える中で、自社の現状と目指すべき姿にはギャップが存在した。その中で、ギャップを解消するために網羅性の高い NIST CSF2.0 を選定し、自社のリスクに応じて重要度の高い項目から戦術を策定した。

解説：

悪いケースでは、経営戦略の実現について全く考慮せず、ガイドラインに書かれている内容をそのまま適用した。この場合、セキュリティ戦術の実現が経営戦略の実現に寄与するか不明である。

一方で、良いケースでは、経営戦略に基づく、セキュリティ戦略、セキュリティ戦術を作成する中で、ガイドラインを選定することで、経営戦略の実現に寄与することが明確である。

例 2：他社依存

悪いケース：

「同業他社が IEC 62443 を活用しているから」という理由で、自社も同じ IEC 62443 を選定した。例 1 と同様に、経営戦略の実現に寄与するか不明である。

良いケース：

自社のセキュリティリスクや生産機器のネットワーク構成を考慮した結果、IEC 62443 のガイドラインを選定した。

解説：

悪いケースでは、同業他社に依存しており、自社の状況を全く考慮していない。選定するガイドラインは、自社の経営戦略実現に寄与する戦術のみならず、ガイドラインの持つ特性や思想に基づく物を選定しなければならない。

良いケースでは、自社のセキュリティリスクのみならず、セキュリティガイドラインの思想(IEC62443 のネットワークモデル)を考慮したうえで選定している。

例示のまとめ：

上記で示した例は、悪いケースと良いケースではどちらともいずれも同じガイドラインを選定している点は共通している。重要なのは「どのガイドラインを選定したか」ではなく、「何故そのガイドラインを選定したか」であり、そのガイドラインを選んだ根拠が戦略実現に寄与しているかである。選定の根拠が、自社の戦略を実現するための手段として明確であれば、そのガイドラインは有効に機能する。

4. 生成 AI のセキュリティ戦術策定への活用

4.1. はじめに

近年、大規模言語モデル(LLM)に代表される生成 AI は、アイデア創出、要点整理、文書作成支援などの知的作業領域で急速に普及している。セキュリティ戦術策定においても、以下のシーンで生成 AI が活用可能と考え本プロジェクトを推進した。

- 経営戦略、DX 戦略など抽象的な情報から、セキュリティ課題の仮説を構築する
- セキュリティ戦略に即した具体的な戦術例や運用案のバリエーションを提示する
- セキュリティガイドラインの内容を整理・抽出し、必要な対策群を網羅する

これにより、策定プロセスの迅速化、網羅性の向上、検討パターンの拡張が期待できる。ただし、生成 AI の出力には限界も存在するため、適切な活用方針と人的補完が前提となる。

4.2. 本プロジェクトでのアプローチ

2 章の通り、経営戦略、セキュリティ戦略、セキュリティ戦術の順番に導き出されるものとなる。そのため、本プロジェクトでも同様に、まず、経営戦略[3]からセキュリティ戦略を作成、その後セキュリティ戦略からセキュリティ戦術の作成を行い、このセキュリティ戦術の評価を行うことで実効性の検証を行った。具体的には以下手順で実施を行った。

4.2.1. 経営戦略からセキュリティ戦略の出力(STEP1)

まず初めにこのセキュリティ戦略を作成するために、経営戦略からセキュリティ戦略を出力する。

このセキュリティ戦略の出力の際、経営戦略は多数存在するため、この上下関係、包含関係を明らかにするために、①経営戦略の中でセキュリティ戦略上の優先順位を作成する、②優先順位を考慮し、経営戦略からセキュリティ戦略を作成するというステップを踏む。

なお、公開情報にのみ基づき、セキュリティ戦略を作成したが、実業務においてはセキュリティ戦略が既に存在している場合は、本項はスキップとする。

プロンプト例：経営戦略からセキュリティ戦略の出力(STEP1)

[3] 経営戦略等とは、企業におけるセキュリティ戦略を作成するにあたりインプットになるものであり、中期経営計画、DX 戦略のみならず、Group Report 等と呼ばれており、かつこれに限らないものである。

※インプットとして中期経営計画、Group Report 等を添付する。

あなたは企業におけるサイバーセキュリティ戦略、戦術の専門家です。
これからセキュリティ戦略を策定します。
添付した資料の中で、セキュリティ戦略上重要な項目を抜き出し、優先順位をつけ、セキュリティ戦略を作成してください。

4.2.2. セキュリティ戦略からセキュリティ戦術の出力(STEP2)

セキュリティ戦略からセキュリティ戦術は導き出されるのは、2 章の通りであり、このためのプロンプトを作成する。ここで、今回は公開情報のみを用いて戦術を作成したため、出来なかったものの、戦略に基づく社内情報を入れることでより実態に即した内容になると考えられる。

プロンプト例：セキュリティ戦略からセキュリティ戦略の出力(STEP2)
※インプットとして、セキュリティ戦略を確認、自社のマニュアル等を添付する。
※今回は公開情報のみ利用したため、添付はできなかった。

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。

4.2.3. セキュリティ戦術の評価(STEP3)

ここまででセキュリティ戦術は完成したものの、これが本当に「実効性のあるセキュリティ戦術」となっているのか評価を行う必要がある。出力されたセキュリティ戦術の評価を行うもののこの評価の際にも生成 AI を活用することで、自動化を果たすことを考えた。

ここで、「実効性のあるセキュリティ戦術」として 5 項目(整合性、適合性、具体性、効果性、実現性)と考え、この観点で評価を行った。ただし、効果性、実現性については企業における具体的なリソース(セキュリティ担当者が何名いるなど)や、セキュリティ戦術を実際に計画に落とした後の振り返りが必要となるため、本文書では評価の対象からは外した。

観点	定義	本文書での評価対象
整合性	経営戦略と論理的に結びついているか	対象
適合性	セキュリティガイドラインと適合しているか	対象
効果性	リスク軽減や監査対応など明確な効果があるか	対象外
具体性	手順に展開可能なレベルで書かれているか	対象
実現性	自社のリソース、体制、成熟度で導入可能であるか	対象外

表 1 セキュリティ戦術の評価観点

この評価観点に基づき、1(全くできていない)～4(完全にできている)の評価を行いプロンプトの改善を繰り返すことでよりよいセキュリティ戦術の策定、のみならずプロンプトの改善、評価指標の考察を行った。

プロンプト例：経営戦略からセキュリティ戦略の出力(STEP3)
※インプットとして、評価指標をアップロードする。

添付した評価指標に基づき、1～4 段階で監査人の目線で評価してください。

4.2.4. セキュリティ戦術の確認と改善 (STEP4)

STEP3 までで評価も含めたセキュリティ戦術の作成は完成した一方で、より実効性を上げるために、評価点が向上するような、セキュリティ戦術の見直し案を生成 AI に作成してもらうこともが可能である。

プロンプト例：セキュリティ戦術の確認と改善 (STEP4)
※インプットとして、評価指標を添付する。

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。

4.2.5. セキュリティガイドラインの参照(STEP5)

STEP4 まででセキュリティ戦術が完成した後、セキュリティガイドラインとの紐づけを実施する。セキュリティガイドラインは、セキュリティ戦術作成において、指針となるものであり、ここまで経営戦略等から導き出された戦術を客観的に確認することができるものである。

プロンプト例：セキュリティガイドラインの参照 (STEP5)

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してください。

4.2.6. 戦術の妥当性を判断(STEP6)

本章は生成 AI を用いないものの、重要な観点であり記述を行う。

ここまでで、生成 AI を用いて、経営戦略や、セキュリティガイドラインに紐づくセキュリティ戦術の作成が完成した。

一方で、生成 AI は与えられた文章等に基づき、確率的に正しいとされる文章を作成するシステムである。そのため、経営戦略やセキュリティガイドラインを確認しつつ、責任者、担当者が妥当性を判断しなければならない。

プロンプトの出力例を下記に示す。
STEP1：
強固なブランドの構築と品質向上という経営戦略に対して、セキュリティ戦略は「インシデント対応とレジリエンス」です。
STEP2：
上記セキュリティ戦略に対して、セキュリティ戦術は、「SOC の強化」です。
STEP3：
上記戦術をインプットした評価指標を用いて評価すると、
整合性は 2、適合性は 1 、具体性は 1 です。
STEP4：
ブランド指標に合わせたＳＯＣ運用
評価結果は、整合性は 4 、適合性は 4 、具体性は 3 です。
STEP5：
上記戦術は、NIST SP800-61 Rev2 に紐づいています。

5.　本プロジェクトを通しての考察

5.1.　セキュリティ戦略と経営戦略

本プロジェクトでは、生成 AI を活用し、ガイドラインから即時にセキュリティ戦術が導き出されることを当初期待していたが、品質が上がらなかった。

戦略・戦術・計画の定義や、セキュリティ戦略・セキュリティ戦術が何から導き出されるのかといった、戦略、戦術の全体像が明確にしないと効果が得られた事がわかった。

特に、本プロジェクトを通してまず、企業におけるセキュリティ戦略は、単独で存在するものではなく、企業全体のミッションやビジョン、そして経営戦略に基づいて策定されるべきものであるとあらためて感じた。セキュリティ戦略も生産戦略や財務戦略といった具体的な機能戦略に落とし込まれるのと同様であり、経営目標の達成に貢献するものでなければならない。

この関係性は 2 章の通り階層構造として捉えることができ、頂点に「ミッション/ビジョン、経営戦略」、その下に具体的な「企業戦略」があり、そこから「セキュリティ戦略（Why：なぜ行うか）」が導出される。さらに、「セキュリティ戦術（How：どのように行うか）」、そして「セキュリティ計画（What：何を行うか）」へと具体化されていく。

これらの要素は相互に連携し、上位の戦略・方針との整合性を保つことが重要となるものである。

これらの考察は経営層や戦略立案に長けている人にとって当たり前のものである一方で、多くの企業、セキュリティ戦略、戦術立案担当者は失念するものであると感じており、あらためて考察、提言として残すものである。

提言(セキュリティ戦略と経営戦略)
経営戦略との連動性：セキュリティ戦略は、経営戦略の達成を支援・推進するものであり、これらから導き出される必要がある。
セキュリティ投資や施策の優先順位付けも、経営上のリスクや目標を考慮して行われる必要がある。
戦略実現への寄与：セキュリティ戦術は、最終的に経営戦略の実現に寄与するべきである。

5.2.　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(どのように行うか)を検討する際に、有効な指針となるものである。一方でセキュリティガイドラインが企業で適切に使われていないことが課題と感じていた。

本プロジェクトを通して、セキュリティガイドラインには効果的に活用するためには、いくつかの重要な留意点(前提思想の理解やカスタマイズ)が存在する物であること認識させられた。特に、サイバーセキュリティのリスクは、業種、事業環境、システム構成など、企業が置かれた状況によって大きく異なり、画一的なガイドラインの適用は必ずしも最適解とは限らないものである。

提言（セキュリティガイドライン）
前提思想の理解： セキュリティガイドラインを選定・利用する際には、そのガイドラインがどのような思想や背景（例：IEC 62443 における Purdue model のような参照モデル）に基づいて作成されたのかを理解する必要がある。
自社状況に応じたカスタマイズ： 選択したガイドラインは、自社の固有のビジネスリスクや環境に応じて、内容を取捨選択したり、解釈を調整したり（読み替え）するなど、積極的にカスタマイズする必要がある。

5.3.　生成 AI によるセキュリティ戦術の策定

ガイドラインを用いた、セキュリティ戦術の策定において、専門知識や時間がかかるという課題があった。当プロジェクトでは、近年注目を浴びている生成 AI の活用に着眼して、効率的、品質確保したセキュリティ戦術の策定ができるか検証した。

結果として生成 AI は、セキュリティ戦術の策定プロセスにおいても活用できる可能性を秘めている一方で、生成 AI 活用に関する注意点も存在すると考えた。

まず、今回の検討（ユースケース）では、経営戦略やセキュリティ戦略といった上位概念を入力情報として、生成 AI がセキュリティ戦術のドラフトを迅速に作成できることが確認できた。また、人間が作成する場合とは異なる視点からのアイデアが提示されることも期待できるものであった。

特に生成 AI は、入力されたデータに基づいて「妥当と考えられる文章を作成する」という仕組みで動作する。これは、迅速なドラフト作成やアイデア出しには有効だが、その出力が常に最適であるとは限らないものであり、4 章での結果として、具体的には以下問題点を感じるものであった。

（1）経営戦略との目的直結性の不足

生成 AI は与えられたキーワードや文脈から一定の整合的な戦術を生成できたが、各戦術が経営戦略に対してどのようなリスクを低減し、どのような価値創出に寄与するかという視点が弱かった。

これは生成 AI の「推論力の限界」に起因しており、インプットした内容以外(企業における暗黙知など)を推論する事は難しいものである。

特に今回、公開情報（経営戦略、一般ガイドライン）に基づき策定を行ったため、企業特有のリスク評価結果（例：資産台帳、脅威リスト、リスクアセスメント結果）を踏まえたカスタマイズができなかった。

生成 AI はあくまで一般的推論に留まるため、企業個別のリスク状況を反映した施策提案は人の手による補完が不可欠である。

（2）セキュリティガイドライン適用深度の不足

セキュリティガイドライン自体は十分に参照できたが、個別ガイドラインの適用細部（例：クラウド特有要件、産業制御システム要件）について、生成 AI は深掘り・使い分けを行う能力に限界があった。特にセキュリティガイドラインの前提となる思想などを理解しているわけではない、という点に注意が必要となる。

以上の通り、生成 AI のセキュリティ戦術作成において、骨組みは作成可能であるが、細かな適合性担保は責任者、担当者による追記、判断が必要である。

提言（生成 AI によるセキュリティ戦術の策定）

人間の評価能力の重要性向上： 生成 AI が作成したセキュリティ戦術案の妥当性や有効性を最終的に評価し、判断を人間が行う必要がある。

そのため、生成 AI の活用が進むほど、セキュリティ企画の責任者や担当者には、出力された内容を鵜呑みにせず、戦略的な観点からその妥当性を吟味し、評価できる能力（戦略的思考）を養う必要がある。

6. 今後の展望

今回のプロジェクトを通じて、生成 AI がセキュリティ戦術の作成に大きく寄与することを確認できた。これまで大きな労力がかかっていた部分を削減することができ、間違いなく今後も活用できるものであると考えている。

一方で、各企業が目指す企業価値や、企業固有リスク、ガイドラインの深堀など生成 AI が不得意とする部分や、ガイドラインそのものの読み込みなど、企業の実情の調査といった点は行わなければならない。

そのため、今回の結果を元に、生成 AI とセキュリティガイドラインを実業務で利用しつつも、リスク評価結果の反映、ビジネスゴール意識の強化、ガイドライン適用範囲の明確化を組み合わせることで、より実効性の高いセキュリティ戦術策定が可能になると考える。

参考文献

[1] 内閣サイバーセキュリティセンター,サイバーセキュリティ戦略の概要, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf
[2] 経済産業省 デジタルトランスフォーメーションの加速に向けた研究会,DX レポート 2, https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation_kasoku/pdf/20201228_3.pdf
[3] 中小企業庁,2023 年版「中小企業白書」 第 1 節　成長に向けた戦略 https://www.chusho.meti.go.jp/pamflet/hakusyo/2023/chusho/b2_1_1.html
[4] 経済産業省, デジタルガバナンス・コード 3.0 ～DX 経営による企業価値向上に向けて～, 2024.
[5] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, 2024.
[6] 経済産業省、独立行政法人 情報処理推進機構, サイバーセキュリティ経営ガイドライン Ver 3.0, 2023.

謝辞

本書の作成にあたり、独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム講師の越島一郎先生、佐々木弘志先生、門林 雄基先生には本書の元となるプロジェクトのメンター・講師として、ご指導・ご助言、ご支援をいただいた。改めて御礼申し上げる。

そして、本書の作成や本プロジェクトを共に実施した、以下メンバーの皆様にも感謝を伝えたい。

【プロジェクトメンバー】

【リーダ】
神納　実良

【サブリーダ】
島崎　剛

【メンバー】
木村　光博
笹谷　遼太郎