戦いの原理・原則とサイバーセキュリティ～概要～

背景

ITに係る技術革新とビジネスモデルの変化により、サイバー攻撃の脅威が増大するとともに、企業を取り巻く環境は複雑化している

IT利活用が前提のビジネスモデルへの変化

システムが使えないとビジネスが成り立たない

あらゆるモノがネットワークにつながる

↓

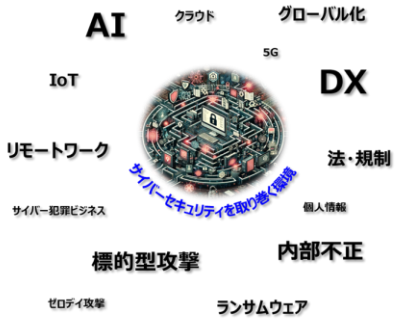
あらゆるモノがサイバー攻撃の影響を受ける

↓

多様化
- 守る物
- 脅威の種類
- 守り方

課題認識

- 「サイバーセキュリティ」そのものを理解せず、個々の知識やスキルを磨いていないか？
- 複雑な環境の中で、組織のリスクに合わせた対応ができているのだろうか？



対応すべき範囲が広がる
- 技術やテクノロジーの教育で手一杯
- 本質的な教育に手が回らない

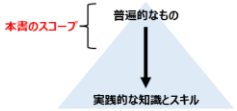
企業のリスクと対応が複雑化
- 何がリスクかわかりづらい
- 全てに対応することはできない

ガイドライン等が世に溢れる
- 何を参照すれば良いか分からない
- 言われるがままに従う

本書の目的

- 企業の複雑なサイバーセキュリティ環境を理解するためのヒントを提供する
- サイバーセキュリティにおける状況判断（ディシジョン・メイキング）のコツを提供する

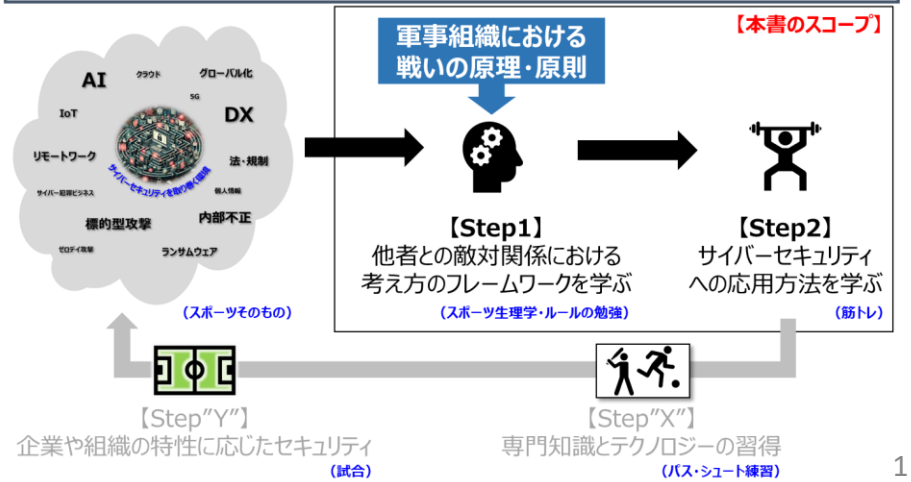
複雑で変化する状況の中で生きていく術



状況を理解する力	溢れかえる情報から、必要な情報を嗅ぎ分ける **“敵対者”のことをもっとよく理解する** →Point！
適切に判断する力	良し／悪し、適切／不適切　の物差し 状況を分析して**意思決定する手順**
行動する力	セキュリティの仕事の現場で活かす

アプローチ

- 軍事組織のバイブルである「戦いの原理・原則」をプロジェクトの拠り所にする
- 他者との敵対関係を有利に進めるための要素と考え方（ロジック）を理解する



戦いの原理・原則とは

- 戦いの原理・原則は、紀元前から現在に至るまで継承されてきたバイブル
- 実戦経験と教訓をもとに改良され続けた「**他者との敵対関係を上手く進めるコツ**」

紀元前
孫氏
戦争を有利に進めるための教えが初めて取りまとめられた

19世紀
戦争論 戦争概論
・軍事学が発達し、普遍的な原理が解明された
・戦いの原則が体系化された
・クラウゼヴィッツ著,戦争論
・ジョミニ著,戦争概論

20世紀～
近代軍事学
・戦いの原則が9項目に整理
・米陸軍野戦教範に採用
・以降、改良が続けられる
・J.F.C.フラー著,戦いの原則,1920
・米国陸軍,野戦教範100-5,1986
・米国陸軍,野戦教範FM3-0,2022

特徴とポイント		
紀元前から脈々と紡がれてきた軍事組織のバイブルである	他者との敵対関係におけるコツが**体系的でシンプル**に整理されている	度重なる戦争の教訓を経て**改良し続けられている**

サイバーセキュリティに適用できる理由

戦いとサイバーセキュリティの間には多くの共通的な側面が存在することから、「戦いの原理・原則」から多くの学びを得ることができる

	①大きな目的のための手段である	②自分と他者の相互作用である	③様々な外部要因が影響する	④チームプレー(組織力)が重要である
戦い	領土問題、宗教問題等に起因した政治的な目的で行われる	利害や意見などの不一致、対立によって起こる	情勢、世論、戦場の地形、気象、などの影響を受ける	部隊の指揮・統率や連携した行動が重要
サイバー	サイバー攻撃などの脅威からビジネスを守る	サイバー攻撃者と企業などの間で起こる	法・規制、ｼｽﾃﾑ・ﾈｯﾄﾜｰｸ構成、ｽﾃｰｸﾎﾙﾀﾞｰなどが関係する	企業、業界、国などが協力して行うことが重要

一方 法則や力学が異なる点も存在
サイバー空間では**物理的な質量の概念**がほとんど発生しない

本書で引用した原理・原則

- 自衛隊・米軍でも採用されているフレームワークから、以下3つの原則を活用した
- シンプルかつ包括的であり、イメージアップが容易である

【共通点】他者との敵対関係を有利に進めるためのシンプルなフレームワーク

情報の構成要素 **METT**（メット）	情報の種類とその構成要素であり、動き方と結果に影響を与えるもの
組織活動と戦法 **戦いの9原則**	敵に勝つ（負けない）ための動き方、戦法と組織統治の方法
アクションの分析と決定方法 **意思決定プロセス**	状況を分析し、組織としてのアクションを決めていくための方法と手順

何が嬉しいか
✓ シンプルで包括的なフレームワークなので、様々な物に適用しやすい
✓ 現実世界の出来事なので、誰でもイメージアップして理解しやすい

METTの概要

他者との敵対関係では以下４要素を明らかにし、それらを総合的に分析してアクションを意思決定していくことが重要（→常に意識できるようになれば勝てる！負けない！）

任務（**M**ission）	目的	• 自組織の活動目的、ビジネス目標 • サイバーセキュリティの目標
敵（**E**nemy）	敵対者	• 敵対者は誰か • どのような能力やリソースを持っているか • 何のために、どのようなサイバー攻撃を行うか
地形・気象（**T**errain）	周辺環境	• 自組織のビジネスプロセス、資産 • システム・ネットワーク構成 • 法規制、ステークホルダー、ビジネス環境などの外的要因
部隊（**T**roop）	自分たち	• 自組織が保有するリソース • セキュリティの能力、機能、成熟度 • 連携する機関、協力ベンダ

戦いの9原則の概要

- 部隊が組織的に行動し、敵に対して優位な態勢を占めるために適合すべき要件であり、勝敗や優劣にも大きな影響を及ぼす。
- 戦闘では組織として統制のとれた行動を行い、我の強みを活かし、敵の弱点を突くことが鉄則。9原則はこれを行うための要件だと言える。
- 攻撃／防御のいずれにも適用できる共通的な概念のようなものであり、これから派生した攻撃／防御それぞれ、また、個々のシチュエーションごとの原則も存在

①	目標	Objective	組織として達成可能な**目標**を確立し、その達成のために努力を集中する
②	主動	Offensive	敵の先手を取り、**主導権**を維持する
③	戦力の集中	Mass	重要なポイントに対しては出し惜しみせず、**戦力を集中的に投入**する
④	兵力の節用	Economy	重要なポイント以外では、リスクを覚悟して**必要最小限の戦力**で戦う
⑤	統一	Unity	指揮・統制系統を**一本化**する
⑥	機動	Maneuver	スピード感を持ち、**臨機応変かつダイナミックに行動**する
⑦	奇襲	Surprise	**敵の意表を突き**、敵が予想していない行動により、対応のいとまを与えない
⑧	保全	Security	敵に**有利な情報を与えない**
⑨	簡明	Simplicity	作戦や行動は**シンプルに**する

敵を知ることの重要性

サイバーセキュリティの業務を行う上では、サイバー攻撃者側の意図や狙い、具体的な攻撃手法などに対する理解が必要不可欠となる

従来の取り組み方

業界ガイドラインやフレームワークを参考にセキュリティ対策を検討

→各ガイドラインやフレームワークで推奨されているセキュリティ対策を参考に対応を検討するのが一般的な取り組み方となる

一方で、脅威となる敵の情報が良くわからず・・

課題
- 各ガイドラインで様々な考え方があり、**何が適切なのかわからない**
- **リソースは有限**で、全部対応することは難しい

本書が目指す取り組み方

防御側によるＭＥＴＴの分析

M：目的と任務	セキュリティの目標 資産を守る・ビジネスを止めない
E：敵の状況	サイバー脅威の把握 ・自組織を狙いそうな敵やその目的 ・敵が行う可能性のある攻撃手法
T：周辺環境	周りを取り巻く環境の把握 法・規制・世界情勢など
T：部隊と友軍	自組織の特性や能力にあたる要素 事業規模やシステム構成の管理

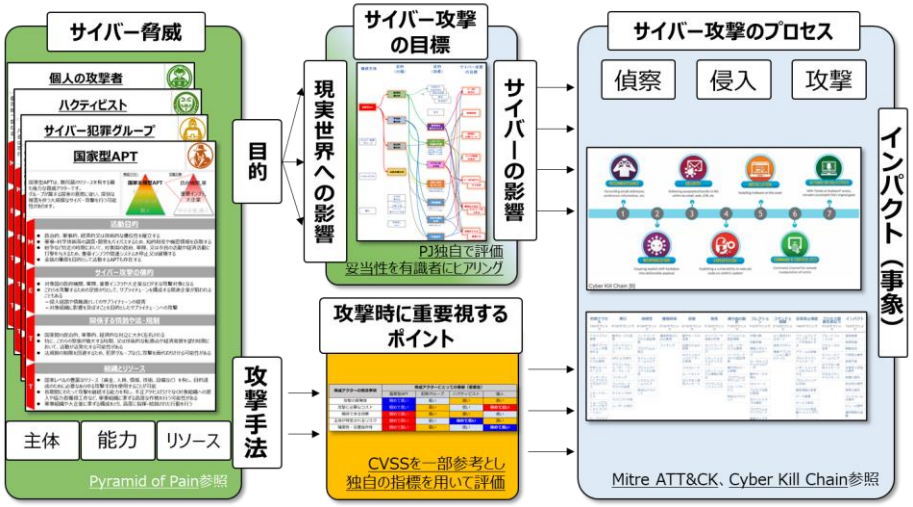
→従来の取り組み方に加え、サイバー攻撃者側の意図や狙い、具体的な攻撃手法を理解することで**「攻撃と防御の全体像」を把握**する

脅威となる敵を具体的に想定することで・・

効果
- それぞれの攻撃手法に応じた**適切な防御策を講じる**ことができる
- **限られたリソースを有効に**活用できる

敵を知るためのアプローチ

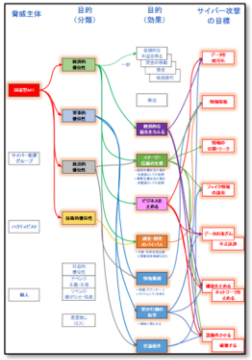
組織の活動背景、メリット・デメリットなどに目を向けることで、分類したサイバー脅威それぞれの背景や活動目的を考察し、選択しうるサイバー攻撃のプロセスを分析した



脅威アクターとサイバー攻撃の目的

○ サイバー攻撃の目的、保有する能力やリソースから、脅威アクターを４つに分類
○ 各脅威アクターが引き起こすサイバー攻撃事象を目的別にマッピング

サイバー攻撃者のMETT（例：国家型APT）



サイバー攻撃者の目的と目標（例：国家型APT）

防御側の教訓

被害・影響の大きさ、深刻度、標的価値は脅威アクターによって異なるため、この違いを認識・理解し、組織のリスクとセキュリティ対策を考えることが重要である

敵にとってのサイバー攻撃手法の「価値」

攻撃者にとってのメリット・デメリットを脅威アクターごとの懸念事項と、攻撃手法ごとの特徴を整理し、敵にとって有利性のある攻撃手法を評価した

脅威アクターにとっての価値		備考
攻撃の容易性	攻撃元区分	CVSS（共通脆弱性評価システム）の一部評価指標を参考とした
	高度なハッキングスキルの必要性	
	特権レベル	
	ユーザ関与度	
攻撃に必要なコスト		戦いの９原則を基に独自の評価指標とした
期待できる効果		
主体が特定されるリスク		
攻撃の確実性		

評価 → 各脅威アクターが重要視する価値

評価 → 各攻撃手法の特徴に基づいた攻撃者にとっての有利性

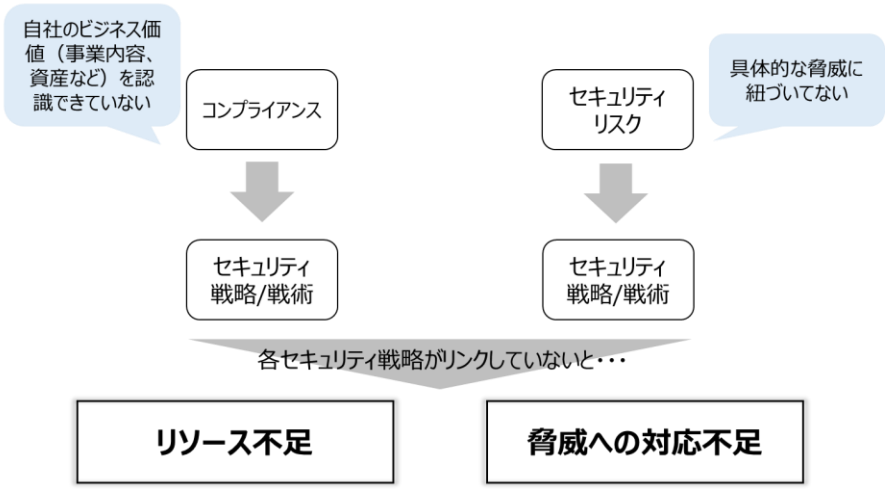
比較

＝

攻撃プロセスで選択される可能性の高い攻撃手法の分析

企業が陥りがちなセキュリティ戦略のミス

自社のビジネス目標や脅威を認識せず、セキュリティ戦略を立てることがある。
その結果、リソース不足や、脅威への対応不足といったことを招く恐れがある。



サイバーセキュリティにおける意思決定のポイント

○軍事組織の意思決定プロセスを参考に、サイバーセキュリティに置き換えて分析
○フェーズごとに、セキュリティ戦略立案においてキーポイントとなる業務を洗いだした

	1：任務の分析	2：作戦環境の分析	3：敵の分析	4：作戦の立案
目標	状況を理解し、達成すべき目標を特定する	戦場の状況など、戦いに影響を及ぼす要因を特定する	敵対者の目標と予想される行動を特定する	ここまでに特定した要因から、今後の行動方針を意思決定する
戦いにおける実施事項	●彼我の目的の分析 ●戦場の特定 ●彼我の戦力の比較 ●作戦方式の決定 ●作戦目標の確立	●地形の分析（重要地形の特定） ●気象の分析（影響と対応の決定）	●敵の目標の分析 ●敵がとり得る行動の列挙・分析 ●各行動の妥当性の評価	●行動方針の列挙 ●行動方針の比較・分析 ●行動方針の決定 ●作戦の立案→実行
サイバーセキュリティに置き換えた場合	●ビジネス目標の分析 ●ビジネスに必要な資産 ●組織に対する脅威の特定 ●セキュリティの目標の確立	●業務プロセス、情報資産、脆弱性の特定 ●セキュリティ態勢の把握 ●保護すべき情報資産の特定	●サイバー攻撃の目標（脅威事象）の特定 ●起こり得るサイバー攻撃シナリオの列挙 ●各シナリオの発生可能性の評価	●セキュリティ対策の列挙、比較、決定 ●セキュリティ対策の実装、運用、（インシデント対応）

リスク分析とセキュリティ対策の関係性

サイバーセキュリティは、**組織全体としてのビジネス目標、脅威、リスクを明確にし、**それに従って演繹的に詳細なリスク分析と対応策の検討を進めることが重要