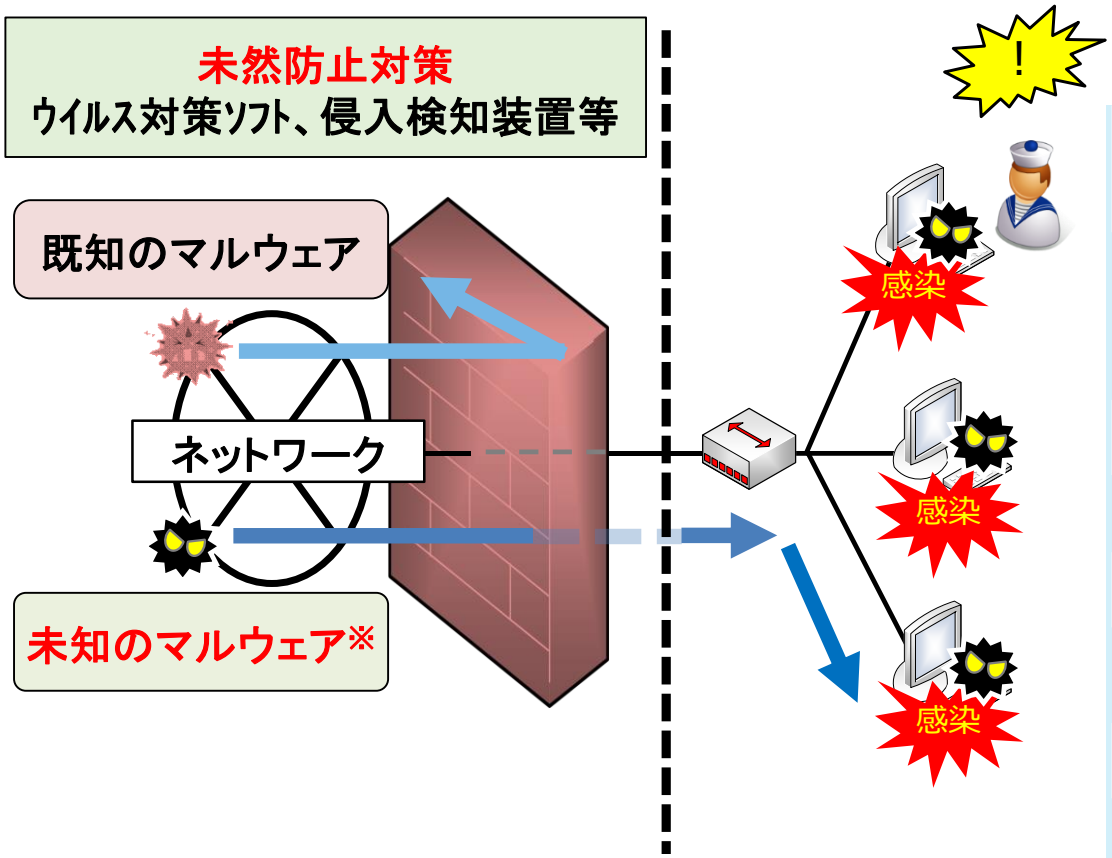
サイバーセキュリティの未来

防衛装備庁
次世代装備研究所　情報通信研究部
サイバーセキュリティ研究室

目次

1. サイバー攻撃対処の考え方(1/2)



未知の攻撃への対応フロー

検知
（気付き）
・普段と異なる振る舞い
・運用者からの報告

分析

判断
・対処方策の決定

制御
・対処方策の実行

任務遂行中は確実に運用を継続させる必要がある！

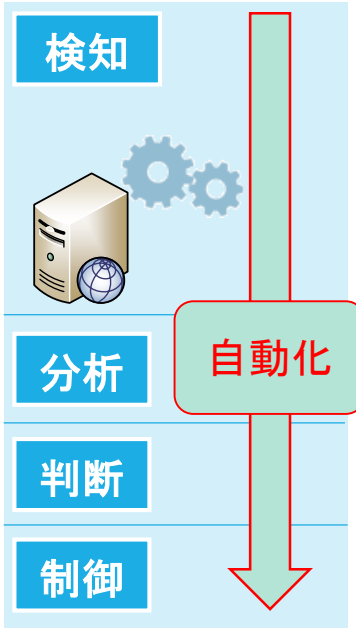
※マルウェア（ Malicious Software） ⇒ 悪意のあるソフトウェア。トロイの木馬、コンピュータウイルス等

1. サイバー攻撃対処の考え方(2/2)

自動対処

一連の**プロセスを自動化**し、迅速な対処を実現

検知から制御まで迅速な自動処理



課 題

日々新たな攻撃手法が作られるため全ての自動対処は困難

人的対処と連携

○サイバーレジリエンス※技術
○未知のサイバー攻撃検知技術

人的対処

各種サイバー攻撃に迅速に対処できる**人材を育成**

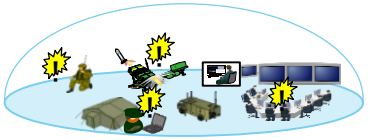
課 題

経験したことがない状況への対処は困難

実機相当環境での演習により能力向上

従来は専門的な知識を有するサイバー防護部隊を対象

作戦に関わる全システムのユーザを対象

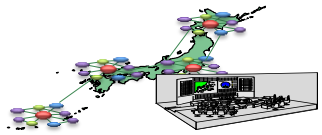
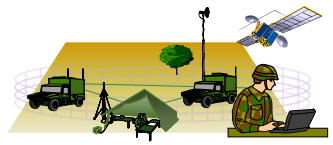


未知の攻撃に対しても、各人が対処能力を発揮

○サイバー演習環境構築技術

※サイバー攻撃等によりシステムの一部が損なわれても、柔軟に対応し運用可能な状態に回復する能力

2. 研究の取り組みについて

システム ＼ サイバー攻撃対策		未然防止対策	運用継続対策		
		既知の脅威	未知の脅威	自動対処	人的対処
クローズ系システム	固定系システム 	マルウェア対策技術、ファイアウォール技術、脆弱性調査技術等	未知のサイバー攻撃検知技術	固定系システム × 自動対処	固定系システム × 人的対処
	移動系システム 			移動系システム × 自動対処	移動系システム × 人的対処
	装備システム 			装備システム用サイバーレジリエンス技術	装備システム × 人的対処

防衛省が主に研究する領域　　本日主にご説明する事業

3. 未知のサイバー攻撃検知技術(1/2)

研究の概要

- 防衛省・自衛隊に対するサイバー攻撃は、従来のサイバー防護技術では検知することが困難な、全く新しい攻撃が行われる可能性が高い
- そのような未知の攻撃を検知可能とするため、民生先進技術であるAIを用いた検知技術を防衛省・自衛隊へ適用するための課題を抽出し、それらの課題を解決するための研究を行う

研究の背景

- 近年、民生において未知のサイバー攻撃を検知可能な技術の研究が進捗しているものの、AI技術の特性上、一定期間、同じ環境における、まとまった学習データが不可欠
- 防衛省・自衛隊のシステム、ネットワークでは、状況によって環境が変化し、一定期間、同じ環境における、まとまった学習データを十分に取得できないことが想定されるため、不足する学習データを補う技術の確立が必要となる

研究の方向性

- 未知のサイバー攻撃検知技術と不足する学習データを補う技術それぞれを確立
- 未知のサイバー攻撃検知技術は民生の先進技術を取込み、不足する学習データを補う技術は主たる課題として解決を目指す

3. 未知のサイバー攻撃検知技術(2/2)

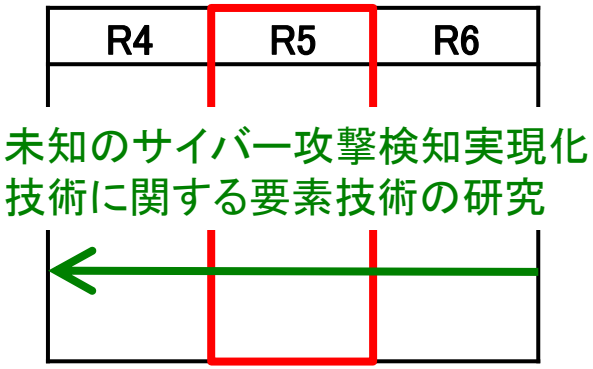
現時点の成果

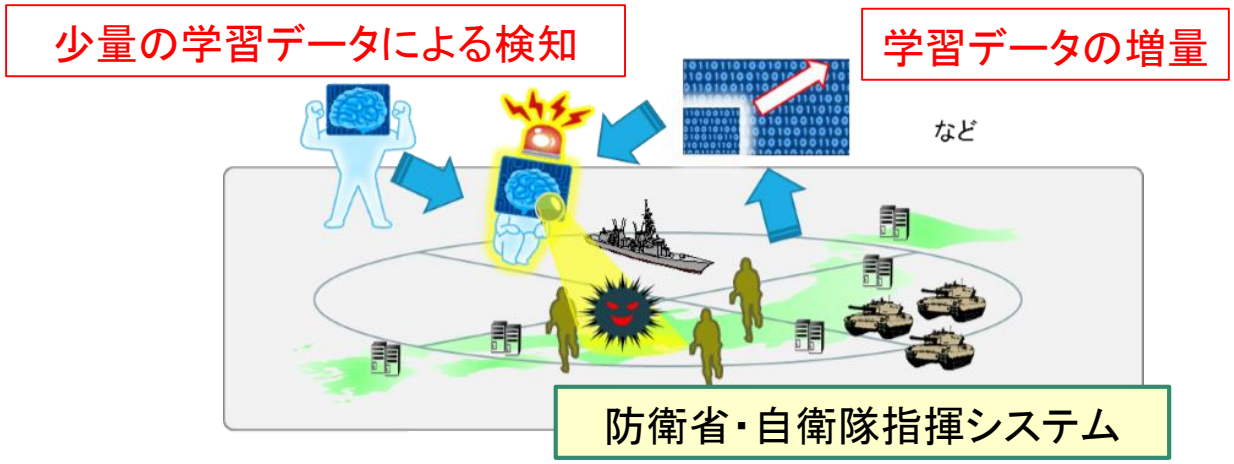
- 未知のサイバー攻撃検知技術について、論文を基に技術を整理し、模擬環境にて検証を実施
- 対象はネットワークにおけるアノマリ検知手法※
- R4時点では、想定したレベルの性能を満足できなかった。

今後の予定

- 実環境にて、未知のサイバー攻撃検知技術及び不足する学習データを補う技術を検証
- 性能向上を目指し、新規技術を取り込むとともに、パラメータ設定等学習方法を効率化
- 性能向上を目指し、ネットワークにおいてAIが検知すべきサイバー攻撃を整理

計画線表





未知のサイバー攻撃の検知用学習データ生成技術の運用構想図

※通常状態を学習することで、通常時とは異なる挙動をしたものを異常と判断する手法

4. 装備システム用サイバーレジリエンス技術(1/3)

研究の概要

- サイバー攻撃発生時等に装備システムの運用継続と被害拡大防止を実現するための装備システム用サイバーレジリエンス技術に関する研究を実施

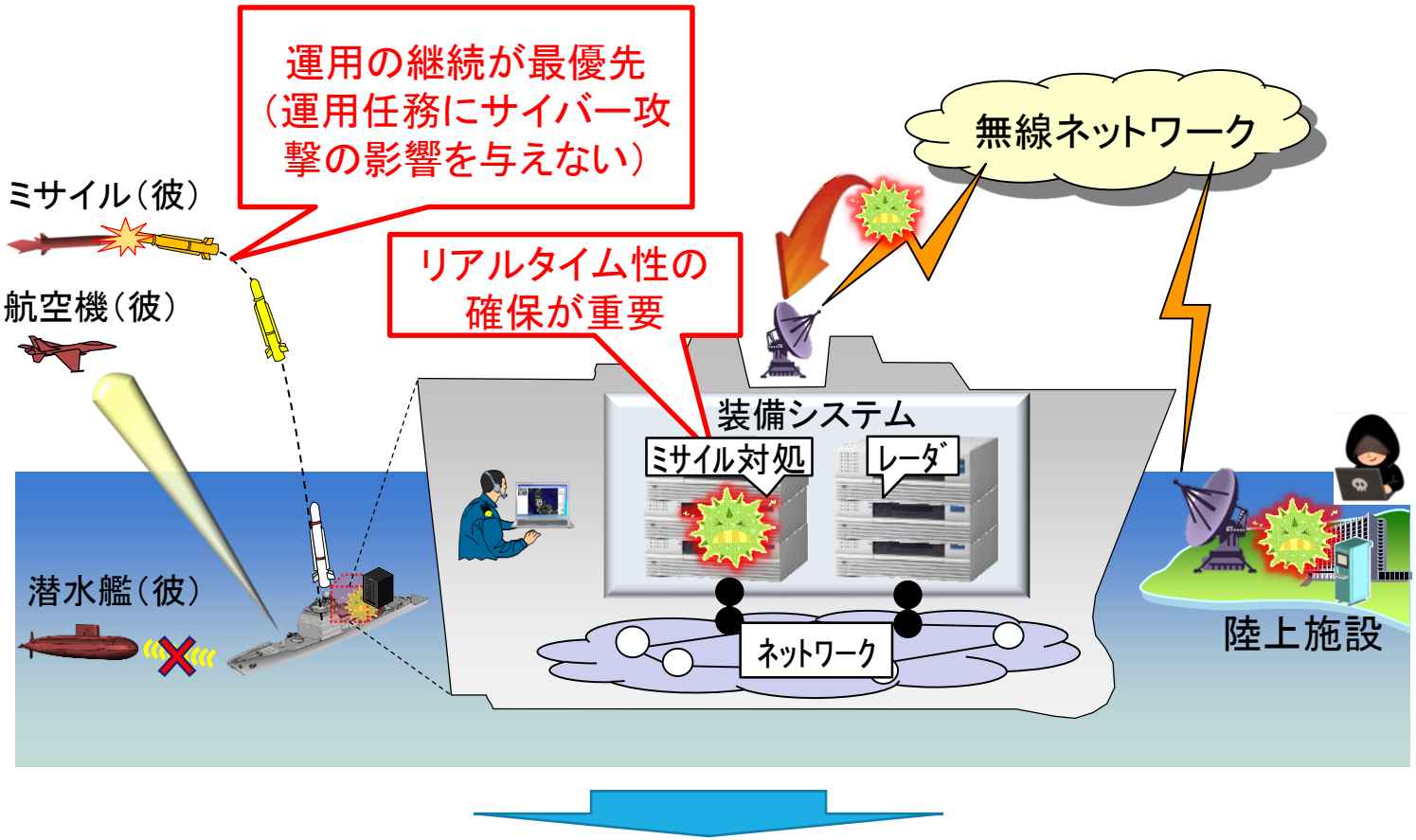
研究の背景

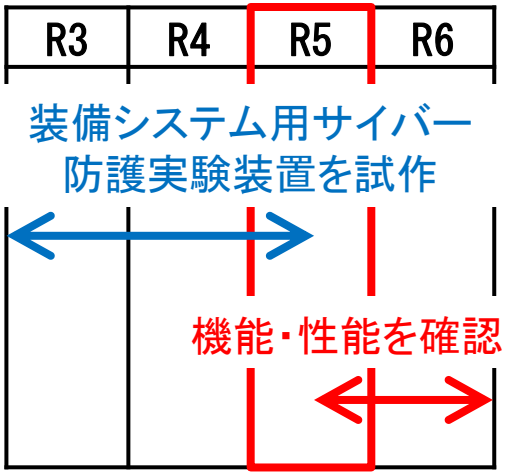
- 装備システムは、その性質上、リアルタイム性※の確保が重要であり、装備システムの機能や処理性能を阻害するなど、装備システムの運用に影響を与えるセキュリティ対策を適用することはできない
- 装備システムはサイバー攻撃を受けた場合においても戦闘を継続する必要があり、運用継続が最優先であるため、サイバー攻撃発生時にサイバー攻撃の被害拡大防止と装備システムの運用継続を両立させる対処を実施する必要がある

※リアルタイム性:求められる時間内にコンピュータの処理が実行できる性質

4. 装備システム用サイバーレジリエンス技術(2/3)

研究の方向性



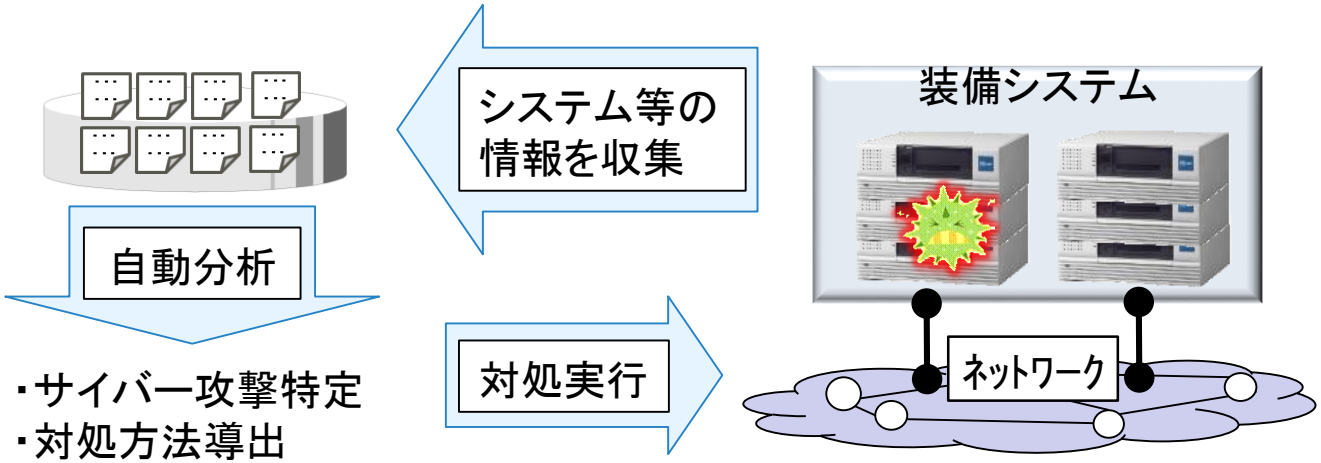


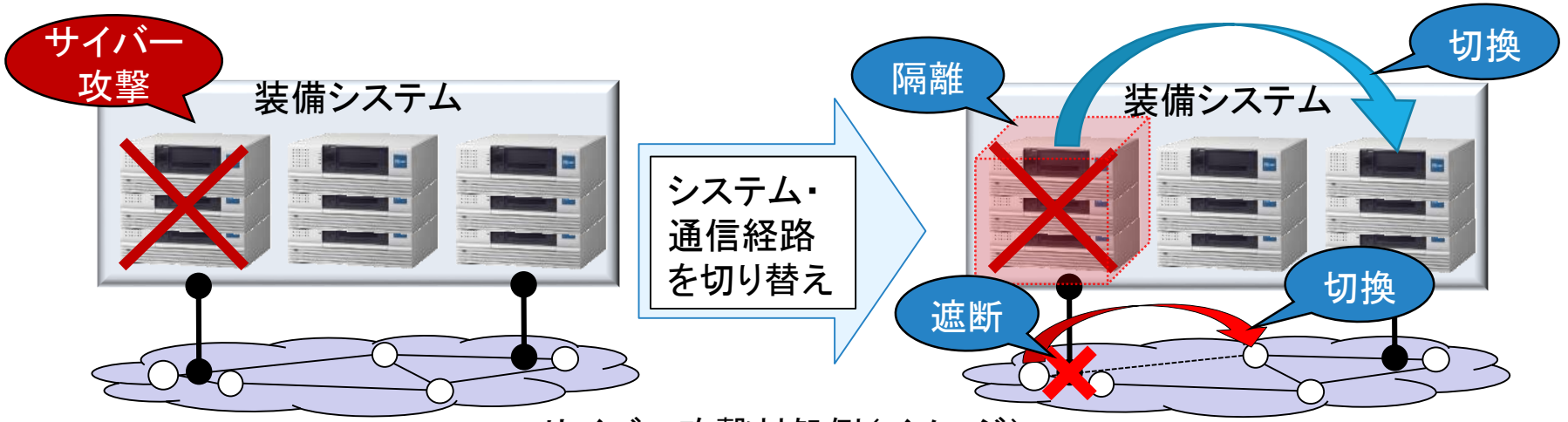
装備システムのリアルタイム性を確保しつつ、サイバー攻撃発生時に被害拡大防止と運用継続を両立させる対処を自動で実施できる仕組みを構築する

4. 装備システム用サイバーレジリエンス技術(3/3)

レジリエンスのイメージ

- システムやネットワークの情報を収集・分析し、サイバー攻撃の特定や対処方法の導出を自動かつ迅速に実施
- サイバー攻撃を受けたシステムの隔離と切換、通信経路の切換をリアルタイムに実施することで、被害拡大防止と運用継続を両立





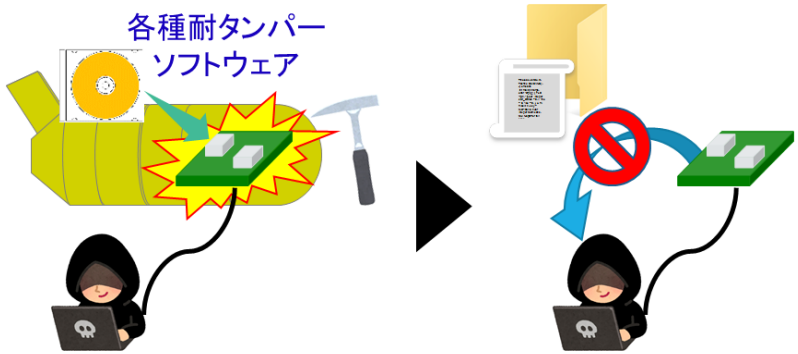
サイバー攻撃対処例(イメージ)

5. その他の研究

ソフトウェア耐タンパー技術

研究の概要

- 防衛装備品に対する不正な解析を防止するため、耐タンパー技術※に関する研究を実施
- 重量や体積の増加、整備性、放熱性の低下等のリスクがない、ソフトウェアの機能による耐タンパー技術を対象としている
- 解析手法の体系的な整理と、ソフトウェア耐タンパー技術の有効性の評価及び実装方法の検討・実証を実施

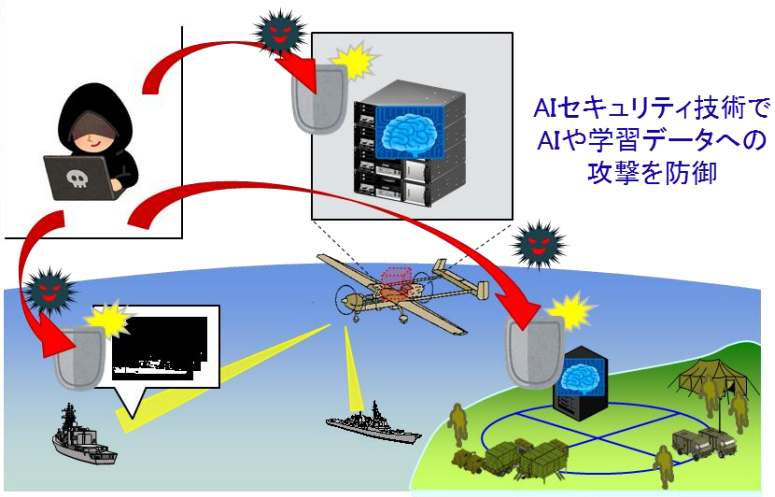


※装備品等の内部に存在する重要情報を、第三者の不正な解析から保護する技術

AIセキュリティ技術

研究の概要

- AI技術の装備化は防衛省・自衛隊において、能力向上等を目的として重点的に推進
- しかし、昨今AIを誤認させるような攻撃が新たに生じる可能性が指摘されている
- そのような攻撃を防ぐため、民生先進技術であるAIセキュリティ技術を防衛省・自衛隊に適用するための課題を抽出し、それらの課題を解決するための研究を行う



6. まとめ

- サイバー攻撃時においても運用継続するため、「未知の脅威への対処」、「自動対処」、「人的対処」の能力向上を目標にしている
- 「未知の脅威への対処」能力向上のため、「未知のサイバー攻撃検知技術」の研究を実施
- 「自動対処」能力向上のため、各システムに適用可能な「サイバーレジリエンス技術」の研究を実施
- 「人的対処」能力向上のため、各システムのユーザが参加できる「サイバー演習環境構築技術」の研究を実施
- その他、「耐タンパー技術」や「AIセキュリティ技術」など、運用継続対策以外の研究も実施