

# サイバーセキュリティ技術の未来

## Future of Cyber Security Technologies

2023年3月

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

青山 貴彦

Cyber Security Research Section

Information and Communication Research Division

Future Capabilities Development Center

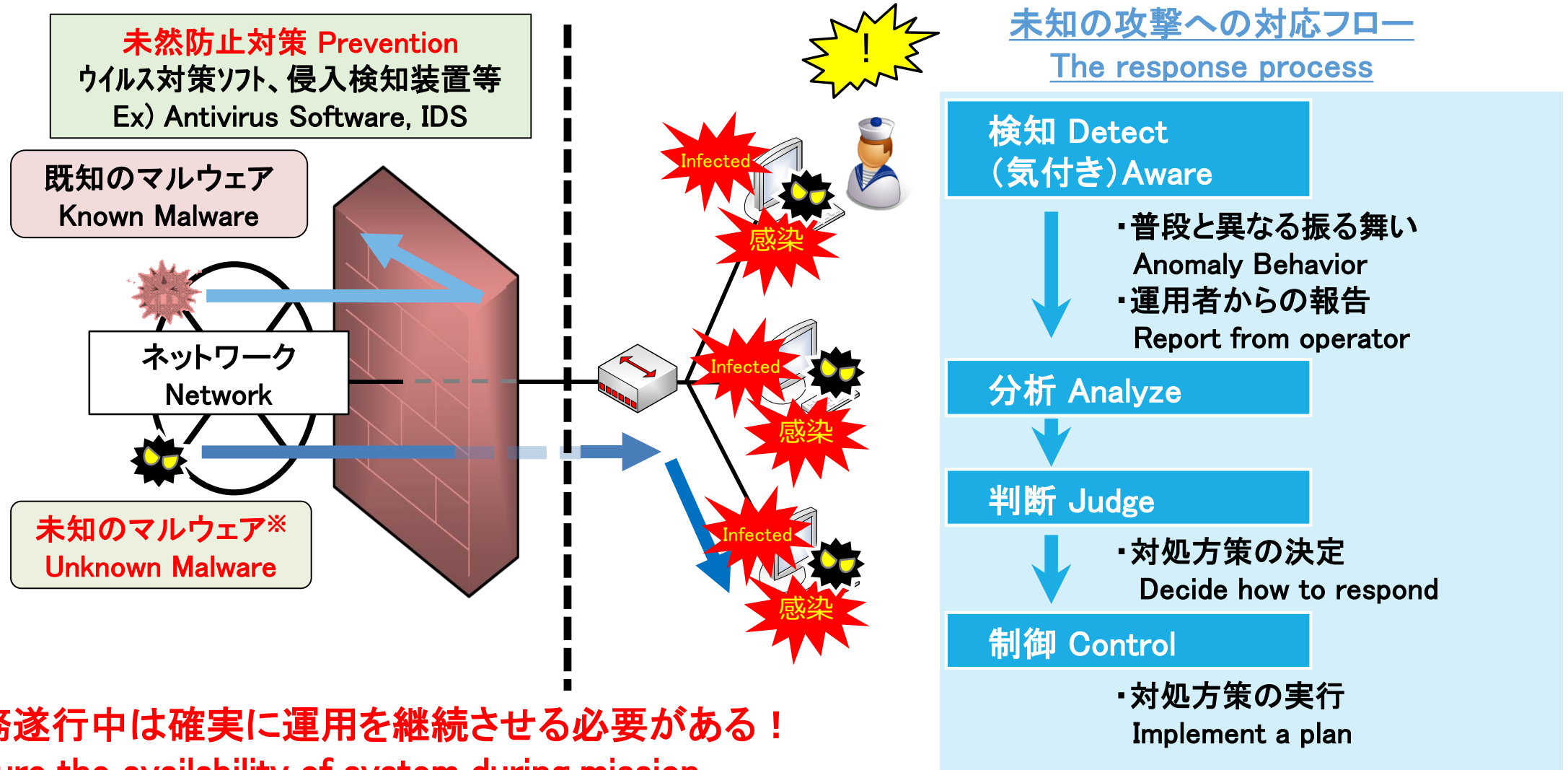
Acquisition, Technology & Logistics Agency

AOYAMA Takahiko

# 目次 Agenda

1. サイバー攻撃対処の考え方  
Countermeasures against cyberattacks
2. 研究の取り組みについて  
Overview of our research
3. 未知のサイバー攻撃の検知技術  
Technology for detecting unknown cyberattacks
4. 装備システム用サイバーレジリエンス技術  
Cyber Resilience Technology for Weapon Control System
5. まとめ  
Conclusion

# 1.サイバー攻撃対処の考え方(1/2)



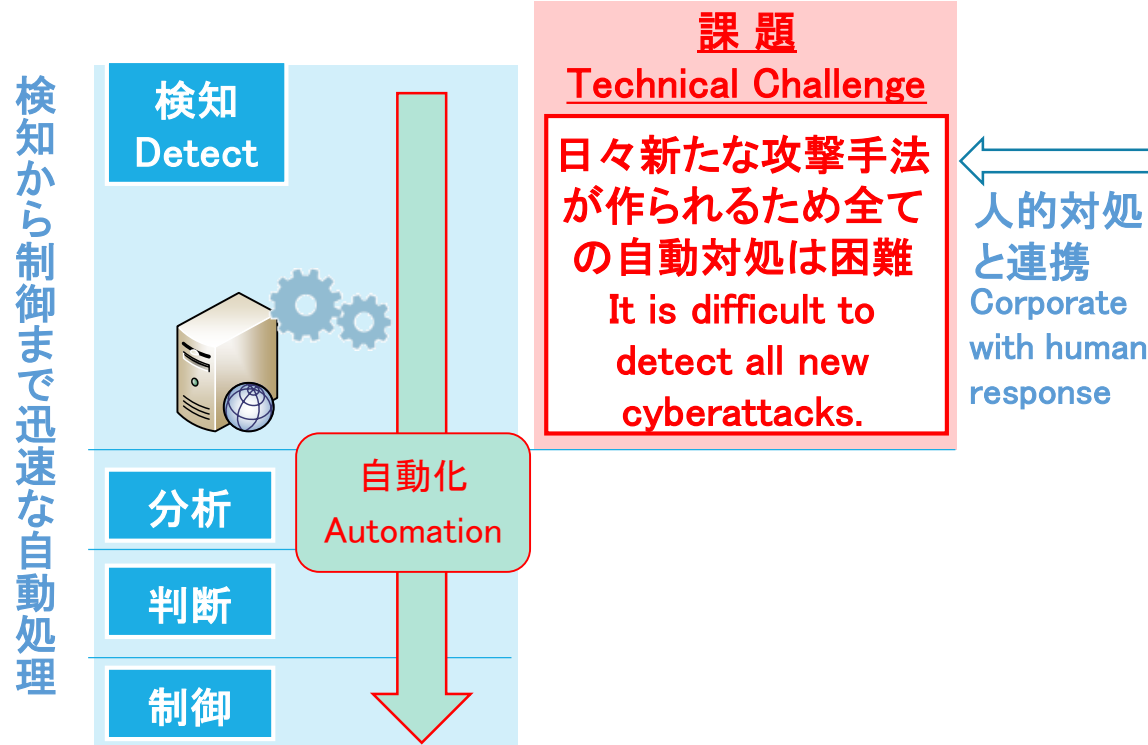
任務遂行中は確実に運用を継続させる必要がある！  
Ensure the availability of system during mission.

※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 Automated Response

一連の**プロセスを自動化**し、迅速な対処を実現  
Automated process can help enhance a quicker response.



- サイバーレジリエンス技術  
Technology for recover from cyberattack quickly and automatically called cyber resilience.
- 未知のサイバー攻撃検知技術  
Technology for detecting unknown cyberattack

## 人的対処 Human Response




各種サイバー攻撃に迅速に対処できる**人材を育成**  
Operators development for quick response against various cyberattacks.



未知の攻撃に対して、各人が検知能力を発揮  
Every operator demonstrate their ability to detect unknown cyberattacks.

- サイバー演習環境構築技術  
Technology for constructing cyber range

## 2.研究の取り組みについて

システム		未然防止対策 Prevention Measures		運用継続対策 Measures for operation continuity	
		サイバー 攻撃対策	既知の脅威 Known threats	未知の脅威 Unknown threats	自動対処 Automatic Response
クローズシステム Closed Systems	固定系システム Fixed/Wired Systems 	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 Antivirus Software, Technology for investigating vulnerability etc..	未知のサイ バー攻撃検知 技術 <u>Technology for detecting unknown cyberattacks</u>	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 Mobile Systems 			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 Weapon Control Systems 			装備システム用サイ バーレジリエン ス*技術 <u>Cyber Resilience Tech. for Weapon Control System</u>	装備システム × 人的対処

※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

防衛省が主に研究する領域

本日は説明する事業

# 3.未知のサイバー攻撃検知技術(1/2)

## 研究の概要

### Outline of Research

- 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

We focus our research on the latest detection technologies that use AI, and how to apply these technologies to the Self Defense Force's systems.

## 研究の背景

### Research Background

- 近年のAI技術の発展により、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

Due to the constant environment changes of the Self Defense Force's systems and networks, it is not possible to collect enough training data.

# 3.未知のサイバー攻撃検知技術(2/2)

## 研究の方向性

Research Directions

- 未知のサイバー攻撃の検知を実現するための手法として、ネットワークにおける“通常状態”を学習データとし、未知を含むサイバー攻撃をアノマリとして検知するアノマリ解析手法を採用  
細部要素技術: AE、GAN、LSTM及びCNN等

We use the anomaly analysis methods such as AE, GAN and LSTM to detect the unknown cyberattacks.

- 少量の学習データによる学習、学習データの増幅、モデルの頑健性向上等により不足する学習データの補完を検討

We will explore ways to supplement insufficient training data by learning with small amounts of training data, amplifying training data, and improving the robustness of the model.

## 計画線表

Project Timeline

FY2022	FY2023	FY2024

未知のサイバー攻撃検知実現化  
技術に関する要素技術の研究

←		
---	--	--

少量の学習データによる検知  
Detection with a small amount of training data

学習データの増量  
Increase training data  
など etc



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  
Conceptual Illustration

# 4. 装備システム用サイバーレジリエンス技術(1/2)

## 研究の概要

### Outline of Research

- 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

We conduct research on cyber resilience technology for Weapon Control Systems to ensure operational continuity and prevent damage escalation when cyber attacks occur.

## 研究の背景

### Research Background

- 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

The Weapon Control Systems must be able to continue to fight even in the event of cyberattacks. Therefore, the continuity of operations becomes the top priority. It is necessary to take the measures for both preventing the spread of damage and ensuring the continuity of Weapon Control Systems' operations when encountering cyberattacks.

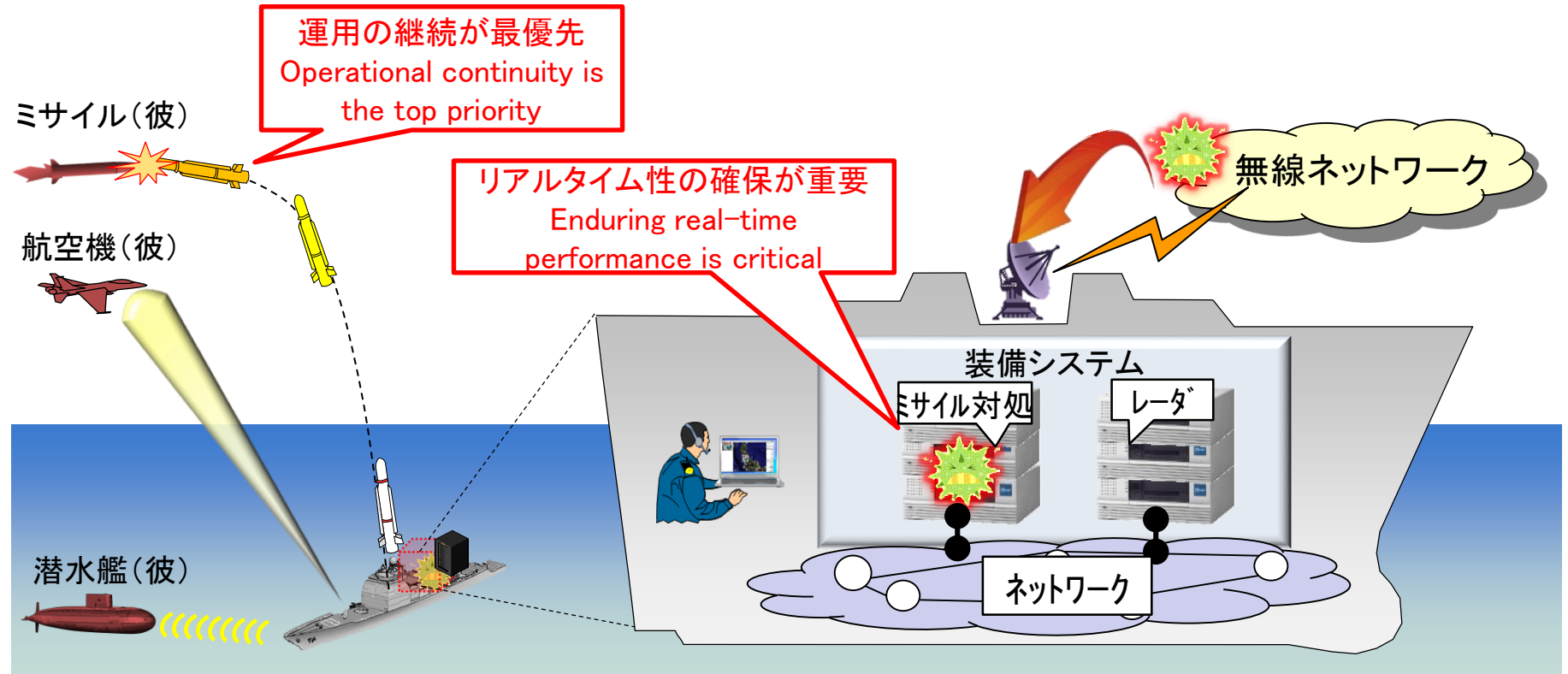
※リアルタイム性: 求められる時間内にコンピュータの処理が実行できる性質



# 4. 装備システム用サイバーレジリエンス技術(2/2)

## 研究の方向性

Research Directions



## 計画線表

Project Timeline

FY2021	FY2022	FY2023	FY2024
装備システム用サイバー防護実験装置を試作			
← 9億 →		← 機能・性能を確認 →	

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応を自動で実施できる仕組みを構築する

Establish a system that can automatically implement measures to both prevent the spread of damage and continue operations in the event of cyberattacks, while ensuring the real-time performance of the equipped system.

## 5.まとめ

- 防衛装備庁では「**未知のサイバー攻撃への対処**」を最重要の課題として、サイバーセキュリティ技術の研究を実施  
ATLA considers the technology for responding to unknown cyberattacks as our top priority.
- **AI技術の活用**により、未知のサイバー攻撃に対する**検知能力の向上**を目指す研究を実施  
We conduct research to improve detection capability against unknown cyberattacks through the use of AI Tech.
- サイバー攻撃発生後の運用継続対策としては、「**自動対処**」と「**人的対処**」の両能力の向上のための研究を実施  
We conduct research to improve both “automatic response” and “human response” capabilities as measures to ensure operational continuity in the event of cyberattacks.
- 「**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  
We conduct research on “cyber resilience technologies” applicable to each system to improve “automatic response” capabilities.
- 「**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  
In order to improve the “human response” capabilities, we conduct research on “constructing cyber range” in which users of each system can participate.