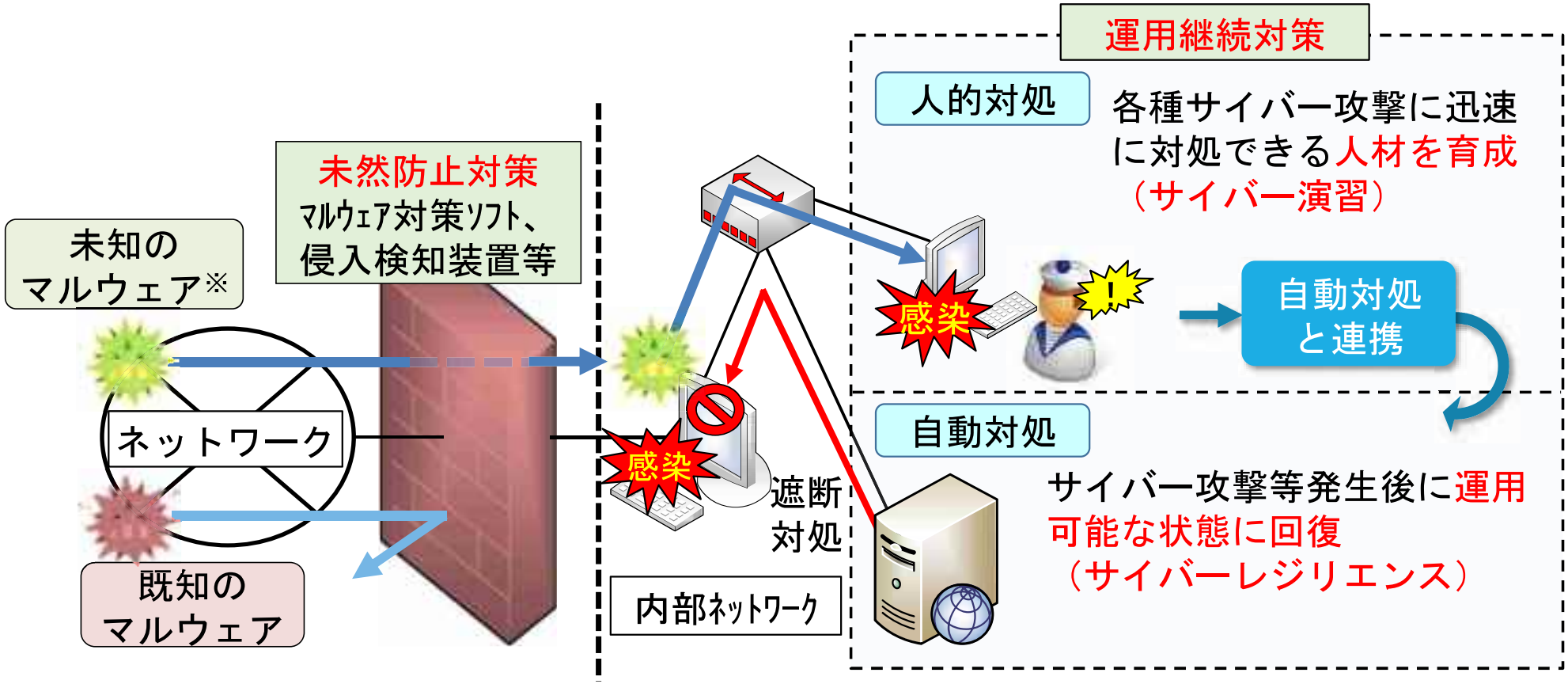
電子装備研究所における
サイバーセキュリティの研究

防衛装備庁 電子装備研究所
情報通信研究部 サイバーセキュリティ研究室
手島　哲郎

サイバー攻撃対処の考え方

➢ 未然防止対策及び運用継続対策（人的対処、自動対処）

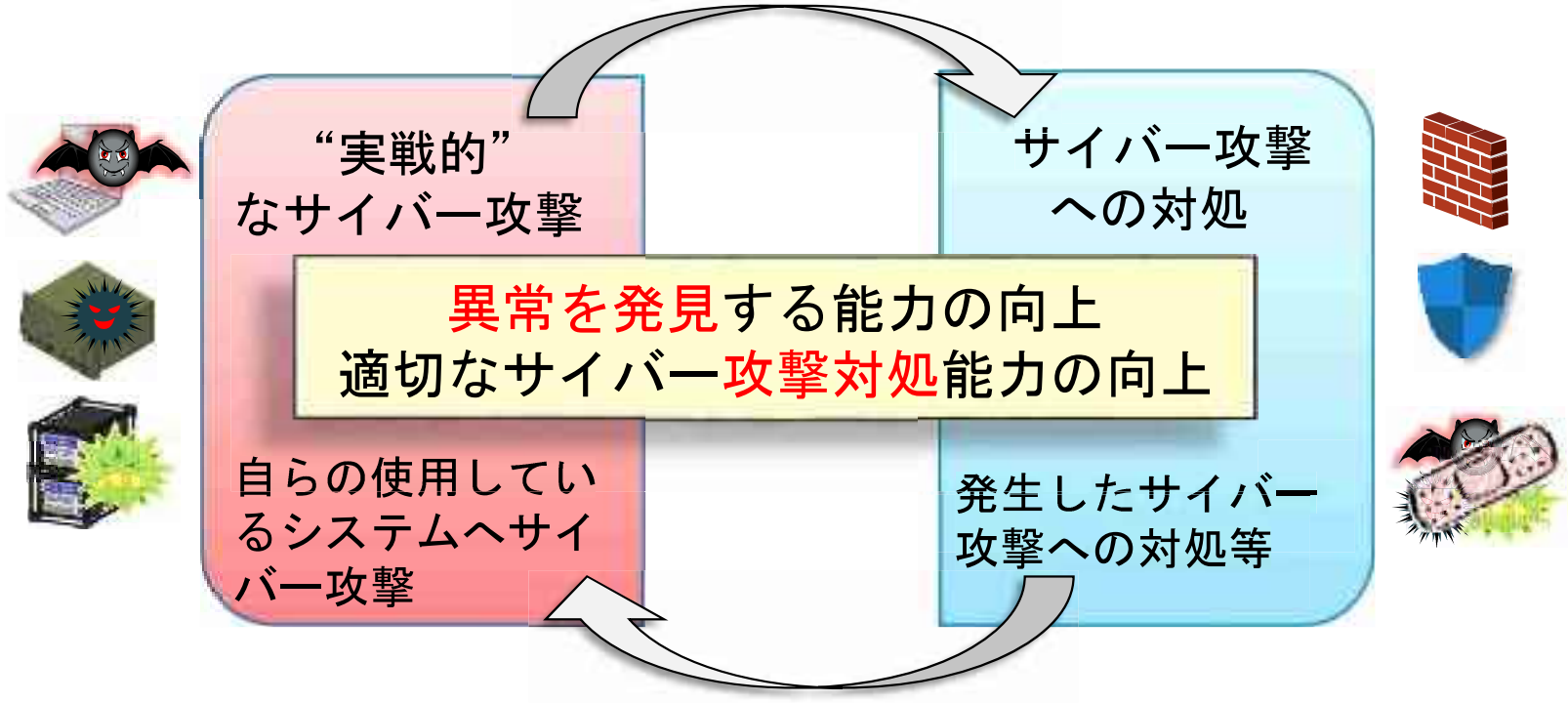


※ Malicious Software ⇒ 悪意のあるソフトウェア。トロイの木馬、コンピュータウイルス等

人的対処の必要性

- サイバー攻撃等発生時にも運用を継続することが必要
- 迅速なシステムの異常検知
- 様々な運用状況における適切なサイバー攻撃対処

日頃から訓練を行いサイバー演習を繰り返すことで…



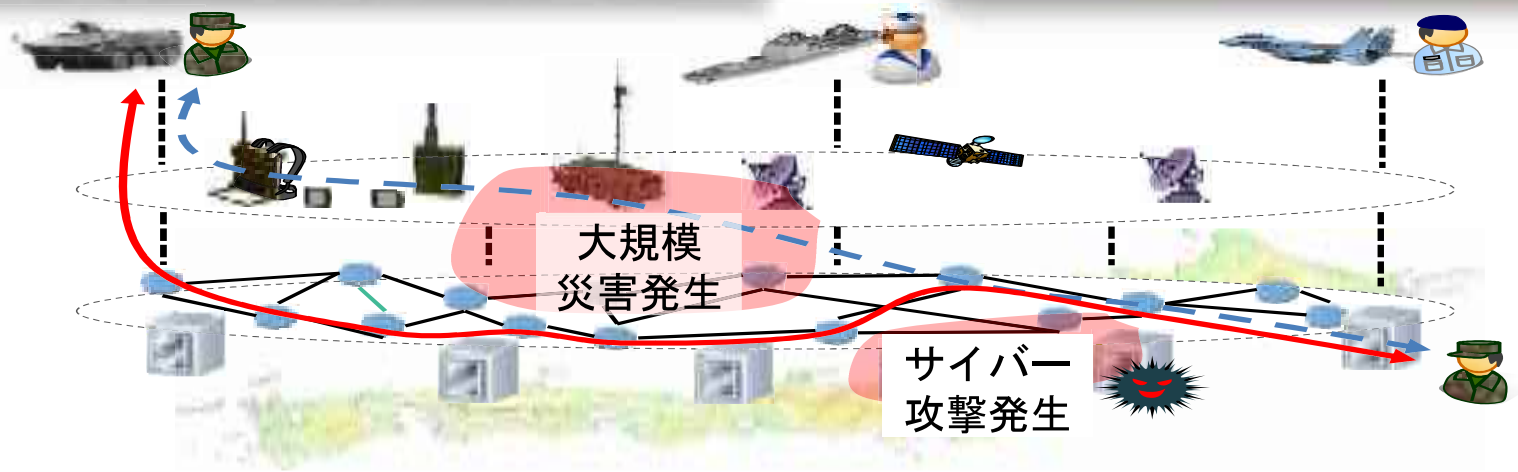
自動対処の必要性

- 大規模なサイバー攻撃、複数拠点の同時破壊等の可能性
- 任務に応じてシステムの優先度が変化

システムの自動対処を実現することで…

複雑な状況においても迅速で適切な対処により運用可能な状態に回復

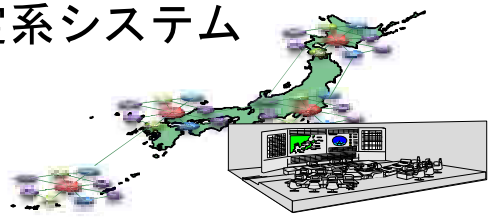
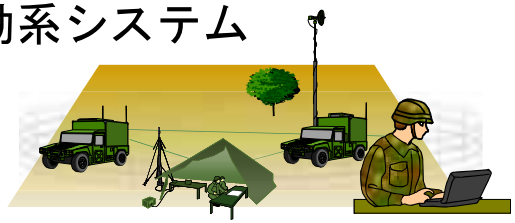
「サイバーレジリエンス」※



※サイバー攻撃等によって、指揮統制システムや情報通信ネットワークの一部が損なわれた場合においても、柔軟に対応して運用可能な状態に回復する能力

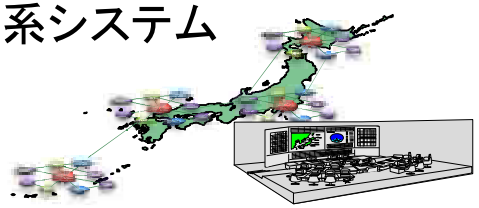
防衛省・自衛隊システムの特徴

➢ 防衛省・自衛隊システムは、インターネットへの接続の有無により、オープン系システムとクローズ系システムに分類

オープン系システム		インターネットに接続されたネットワークで構成
クローズ系システム	固定系システム 	基地内で用いる • 主に民生品と有線ネットワークで構成 • ネットワークの速度は高速で安定的
	移動系システム 	野外に展開して用いる • 主に無線機等の専用品と無線ネットワークで構成 • ネットワークの速度は低速で不安定
	装備システム 	ビークル内で用いる • 専用品と有線ネットワークで構成 • 各装備システムは無線ネットワーク等で連接

サイバー攻撃対処の研究開発の必要性

➢ 主にクローズ系システムの未然防止対策及び運用継続対策に関する研究を実施

システム系＼対策方針		未然防止対策	運用継続対策	
			人的対処	自動対処
クローズ系システム	固定系システム 	ウイルス対策技術、ファイアーウォール技術、脆弱性調査技術、耐タンパー技術等	サイバー演習環境構築技術（H25～H29）	サイバーレジリエンス技術（H29～R2）
	移動系システム 		移動系サイバー演習環境構築技術（H30～R3）	移動系サイバーレジリエンス技術
	装備システム 		装備システム用サイバー防護技術	

防衛省が主に研究する領域

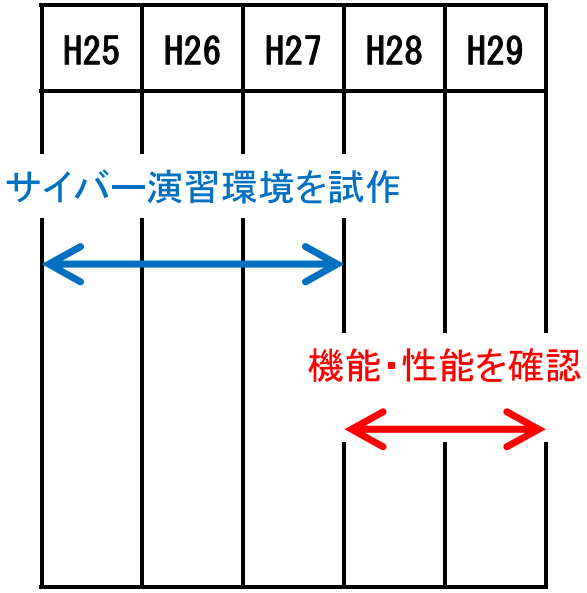
サイバー演習環境構築技術の研究

運用継続対策（人的対処） 固定系システム

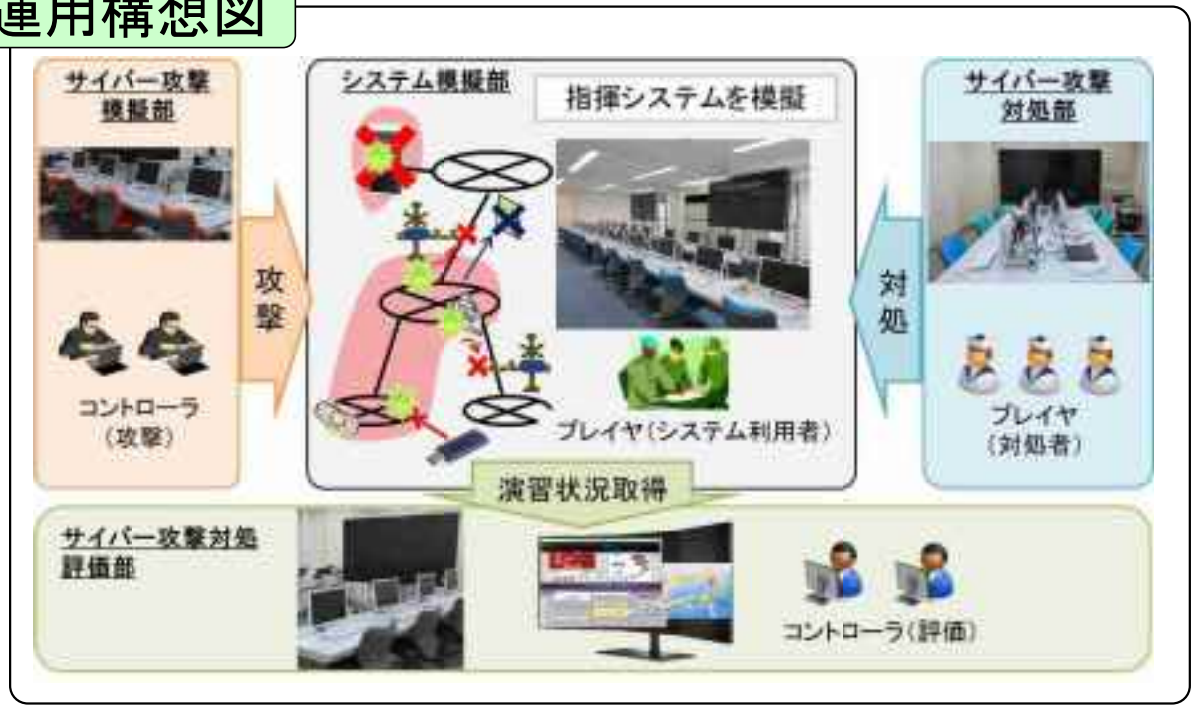
研究の概要

防衛省・自衛隊の固定系の指揮システムを標的としたサイバー攻撃への対処について効果検証等を行うサイバー演習環境構築技術に関する研究を実施

計画線表



運用構想図



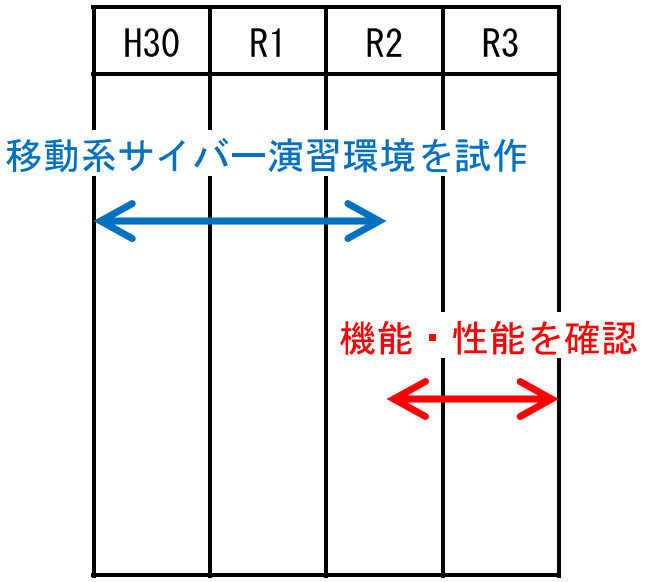
移動系サイバー演習環境構築技術の研究

運用継続対策（人的対処）　移動系システム

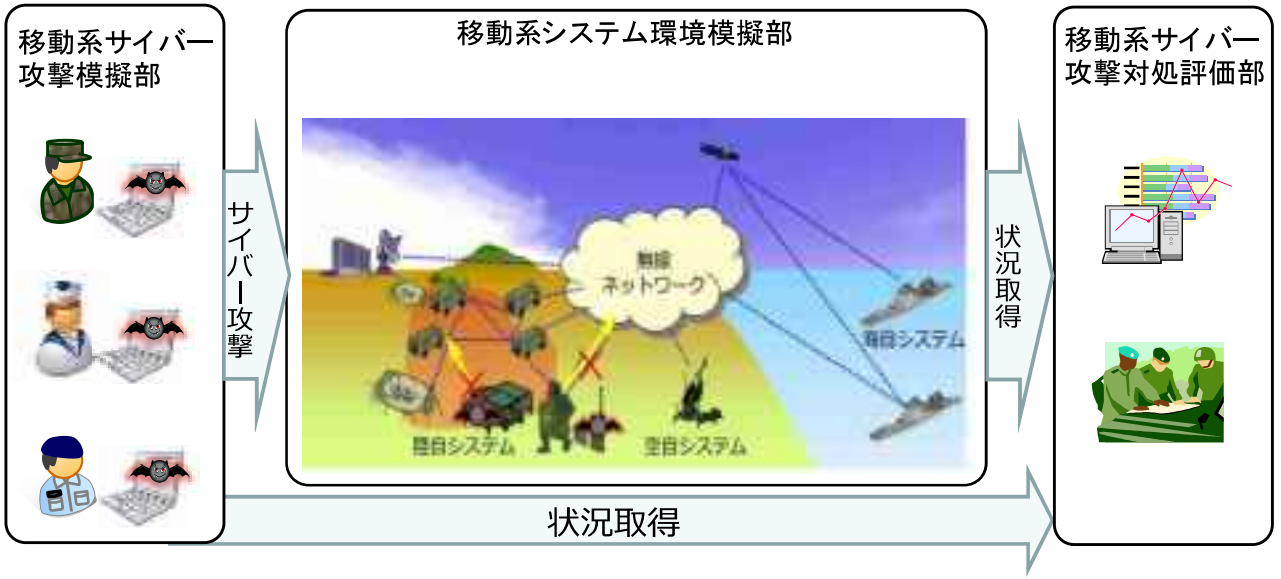
研究の概要

防衛省・自衛隊の移動系システムを標的としたサイバー攻撃への対処について効果検証等を行う移動系サイバー演習環境構築技術に関する研究を実施

計画線表



運用構想図



成果の反映

運用継続対策（人的対処） | 固定系システム | 移動系システム

➢ 研究成果を将来の防衛省・自衛隊のサイバー演習環境の設計等に反映

サイバー演習環境構築技術
（Ｈ２５～Ｈ２９）

固定系システム

固定系の指揮システムを模擬した環境によりサイバー攻撃への対処について効果検証等を行うサイバー演習環境構築技術を実現

成果反映

固定系システムのサイバー演習環境

移動系サイバー演習環境構築技術
（Ｈ３０～Ｒ３）

移動系システム

攻撃模擬部と対処評価部を実システムに接続することによるサイバー演習の実施を目指す

成果反映

移動系システムのサイバー演習環境

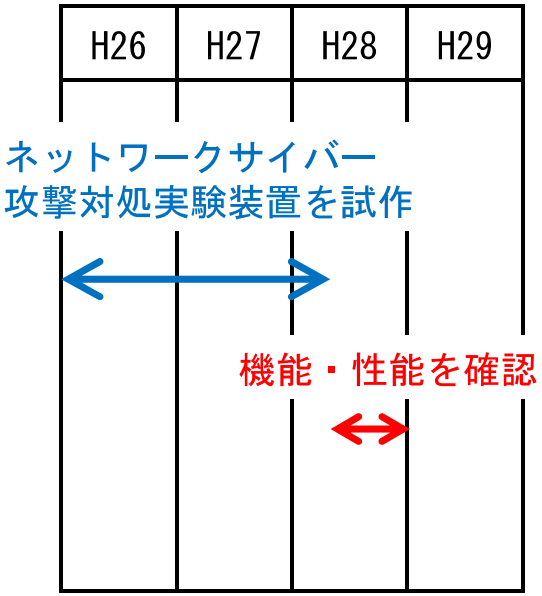
ネットワークサイバー攻撃対処技術の研究

運用継続対策（自動対処） 固定系システム

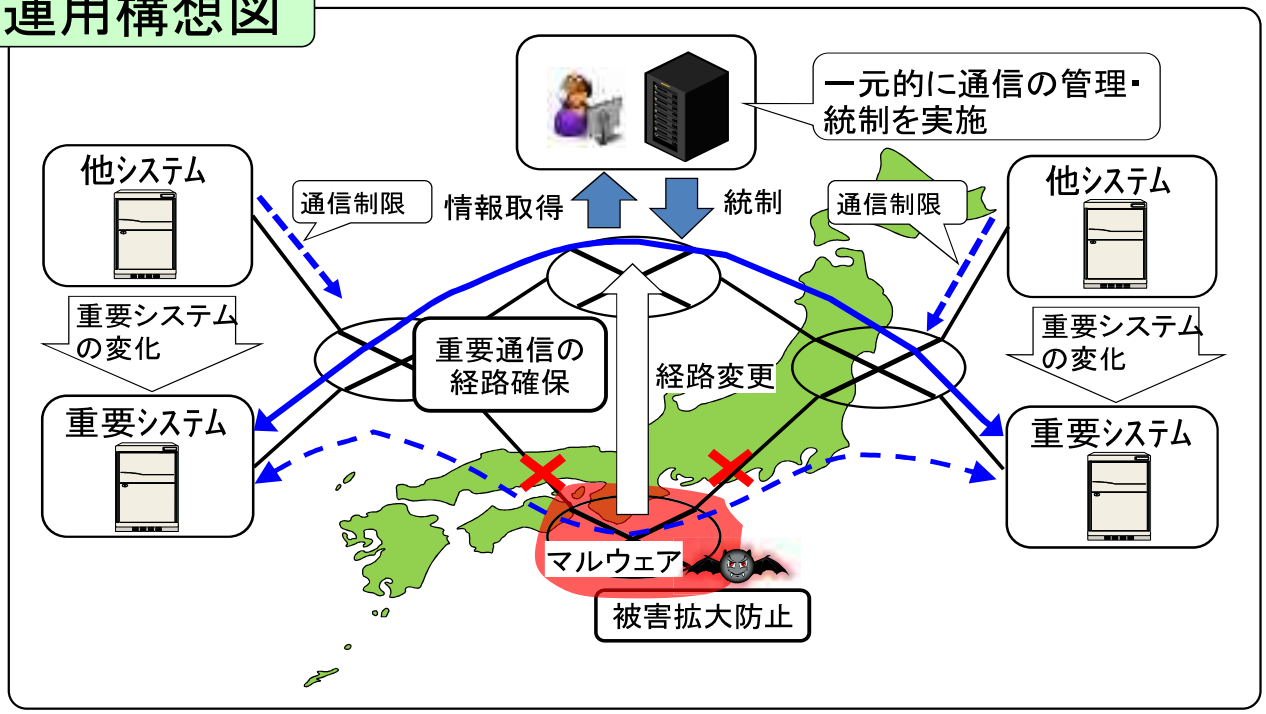
研究の概要

サイバー攻撃発生時等において、防衛省・自衛隊のネットワークの安定的・効果的利用を維持し、任務を遂行するために、重要通信の経路確保と被害拡大防止を行うサイバー攻撃対処等に関する研究を実施

計画線表



運用構想図



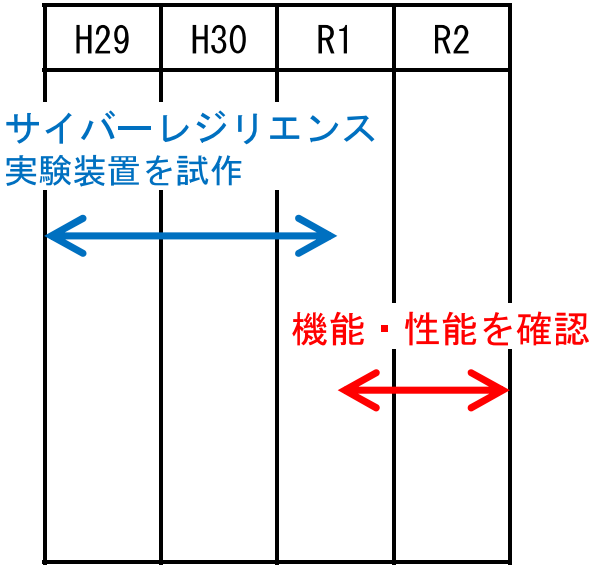
サイバーレジリエンス技術の研究

運用継続対策（自動対処） 固定系システム

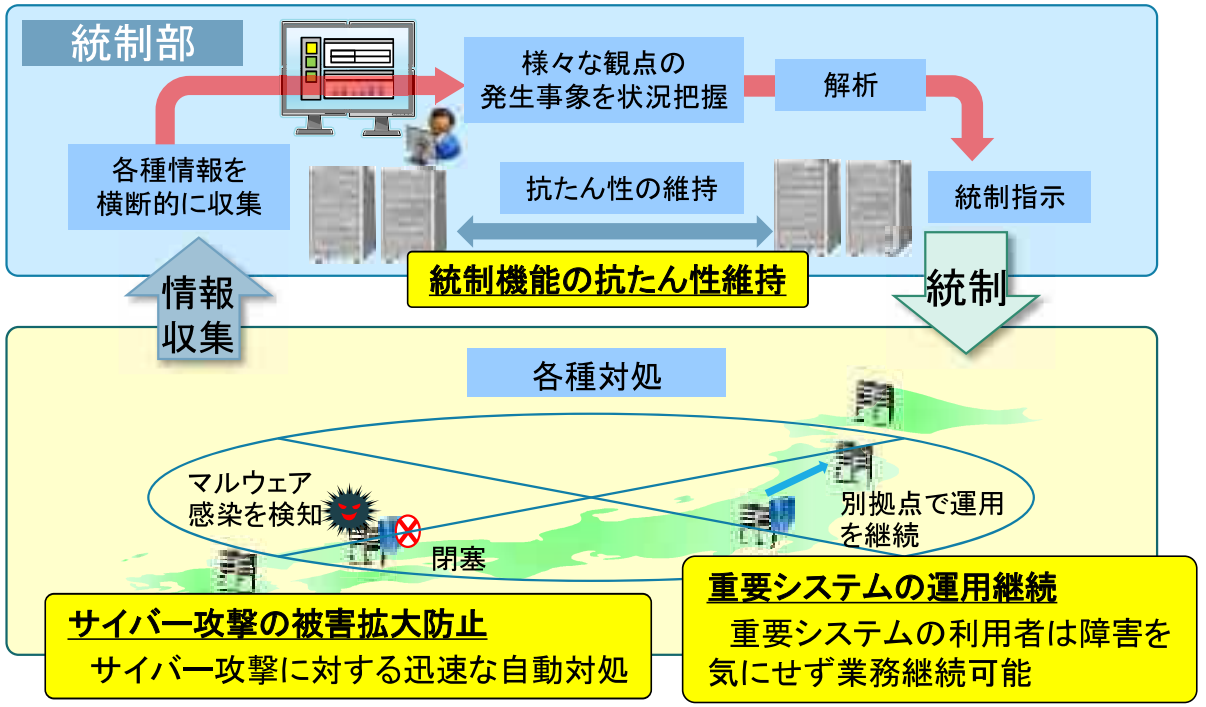
研究の概要

サイバー攻撃や物理的破壊及び障害発生時等に、部隊運用継続を図るため、重要システムの運用継続と被害拡大防止を実現するためのサイバーレジリエンス技術に関する研究を実施

計画線表



運用構想図



成果の反映

運用継続対策（自動対処）

固定系システム

➢ 研究成果を将来の防衛省クラウド環境の設計等に反映

ネットワークサイバー技術
（Ｈ２６～Ｈ２８）

固定系ネットワーク

ネットワーク基盤が被害を受けた場合でも、重要通信の経路確保を実現

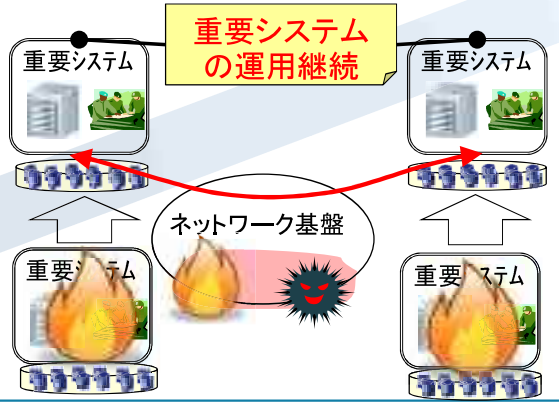
成果反映

防衛省・自衛隊の
ネットワーク環境

サイバーレジリエンス技術
（Ｈ２９～Ｒ２）

固定系ネットワーク ＋ システム

重要通信の経路確保
＋重要システムの運用継続



成果反映

防衛省・自衛隊の
クラウド環境

移動系サイバーレジリエンス技術の研究

運用継続対策（自動対処）　移動系システム

研究の方向性

防衛省・自衛隊の移動系システムに対して、サイバー攻撃や物理的破壊及び障害発生時等に、部隊運用継続を図るため、重要システムの運用継続と被害拡大防止を実現し、サイバーレジリエンスを高めるための移動系サイバーレジリエンス技術を確立する。

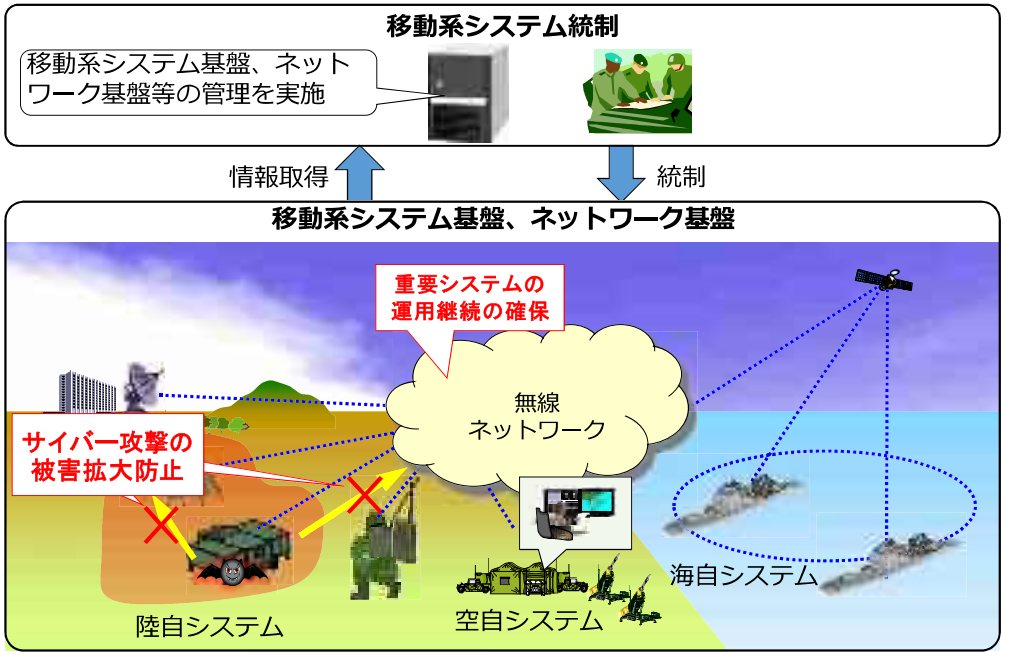
運用構想図

■情報取得

速度・安定性に制約のあるネットワークにおいて、インシデント発生等の情報を取得

■統制

状況に応じてネットワークを統制し、サイバー攻撃の被害拡大防止等を実施



装備システム用サイバー防護システムの研究

未然防止対策・運用継続対策　装備システム

研究の概要

装備システムを標的としたサイバー攻撃への防衛能力を強化するため、サイバー防護技術及びサイバーレジリエンス技術を確立する。

研究の方向性

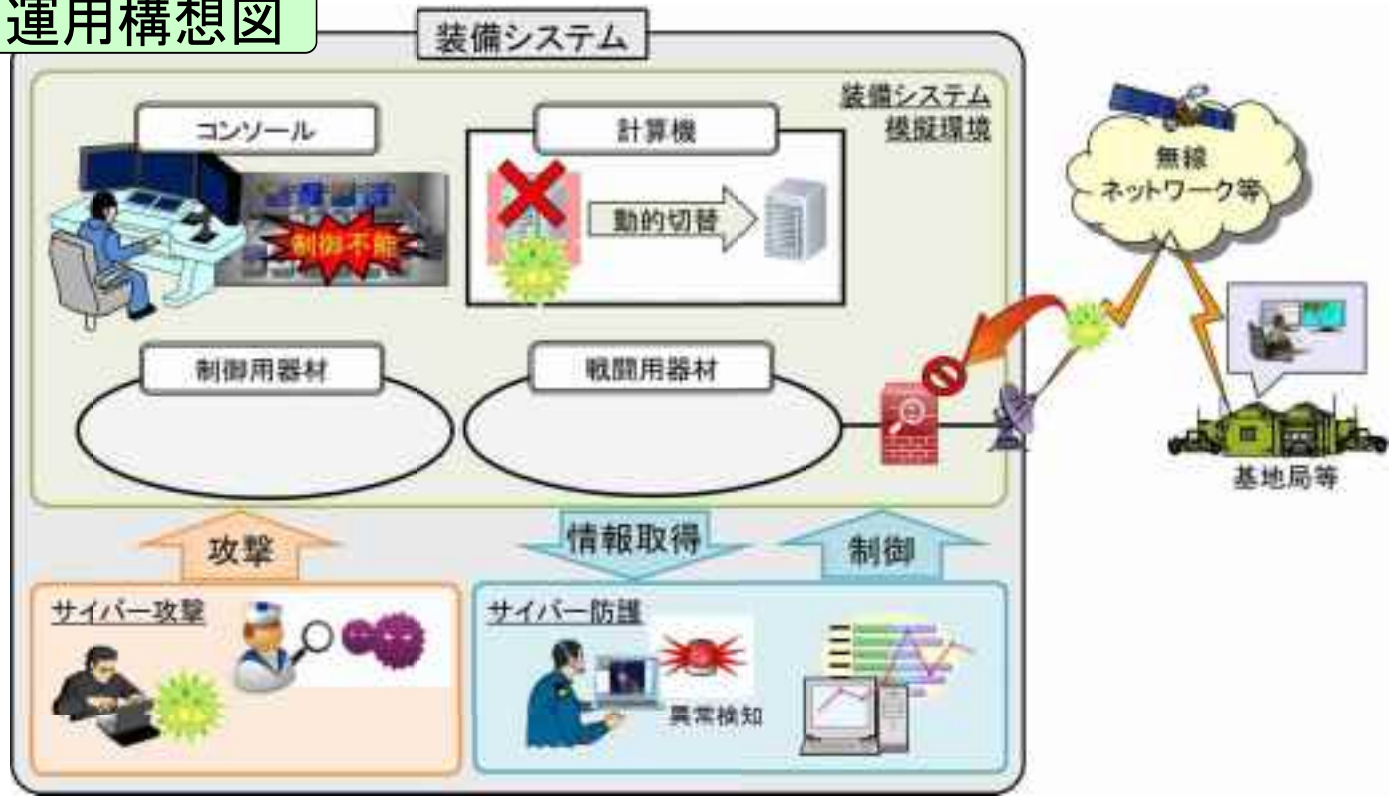
統一的な技術基準が適用されない

多様なプラットフォーム・要求性能

装備システムに対して影響が大きい脅威の分析、対策手法について評価検証

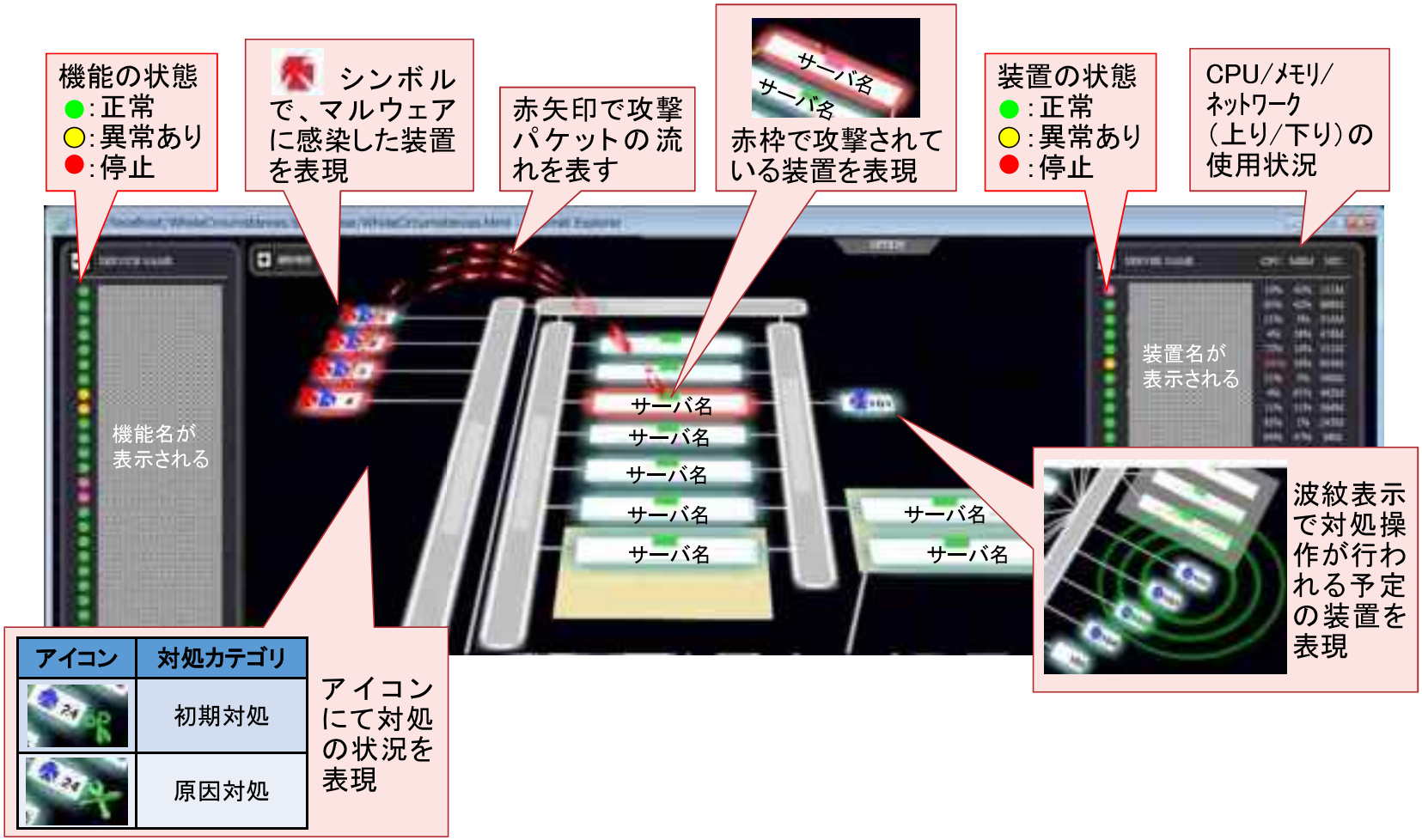
技術基準作成のベース

運用構想図

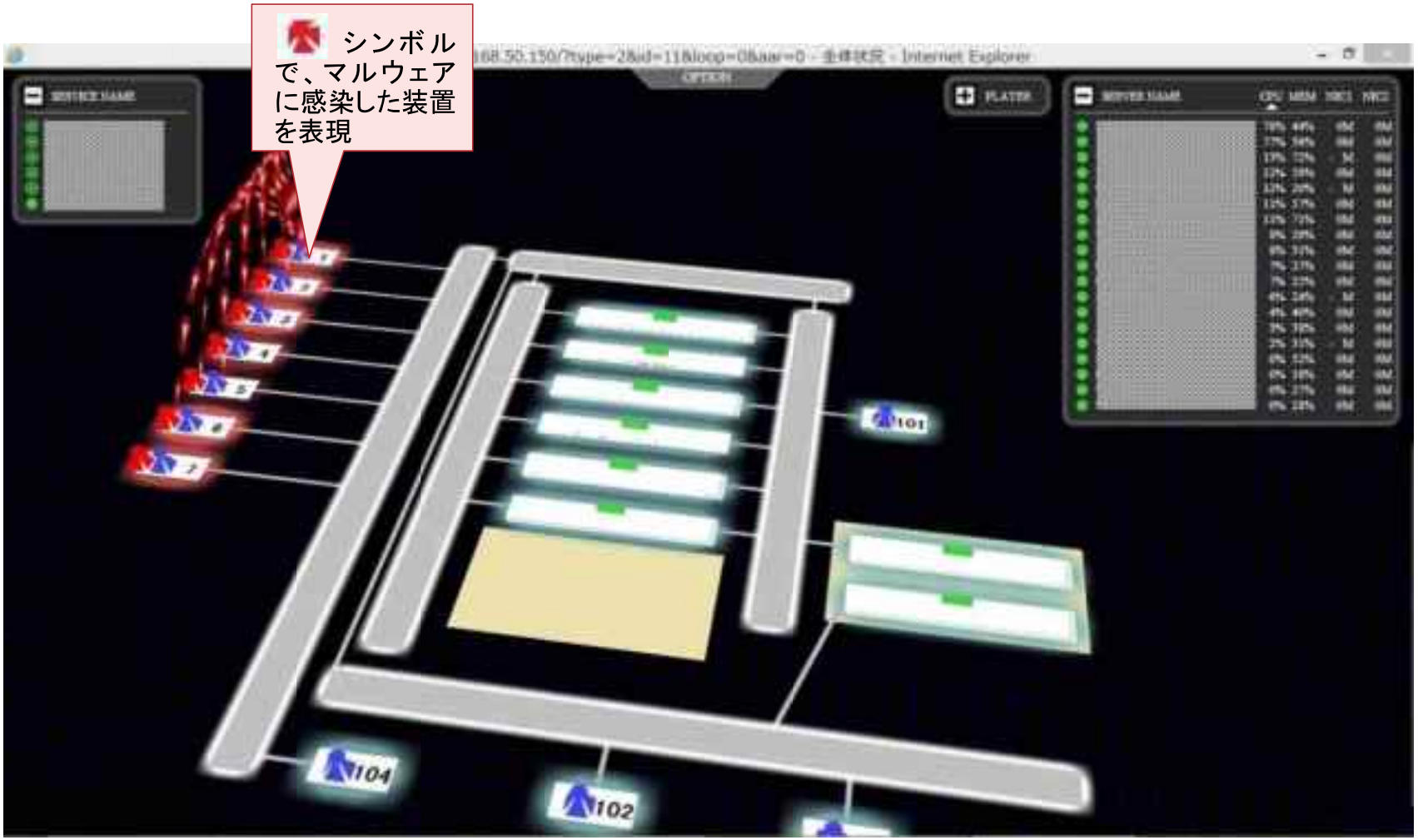


研究成果：サイバー演習環境構築技術（１/５）

演習統制者の意思決定及び状況判断に必要な情報の可視化が可能

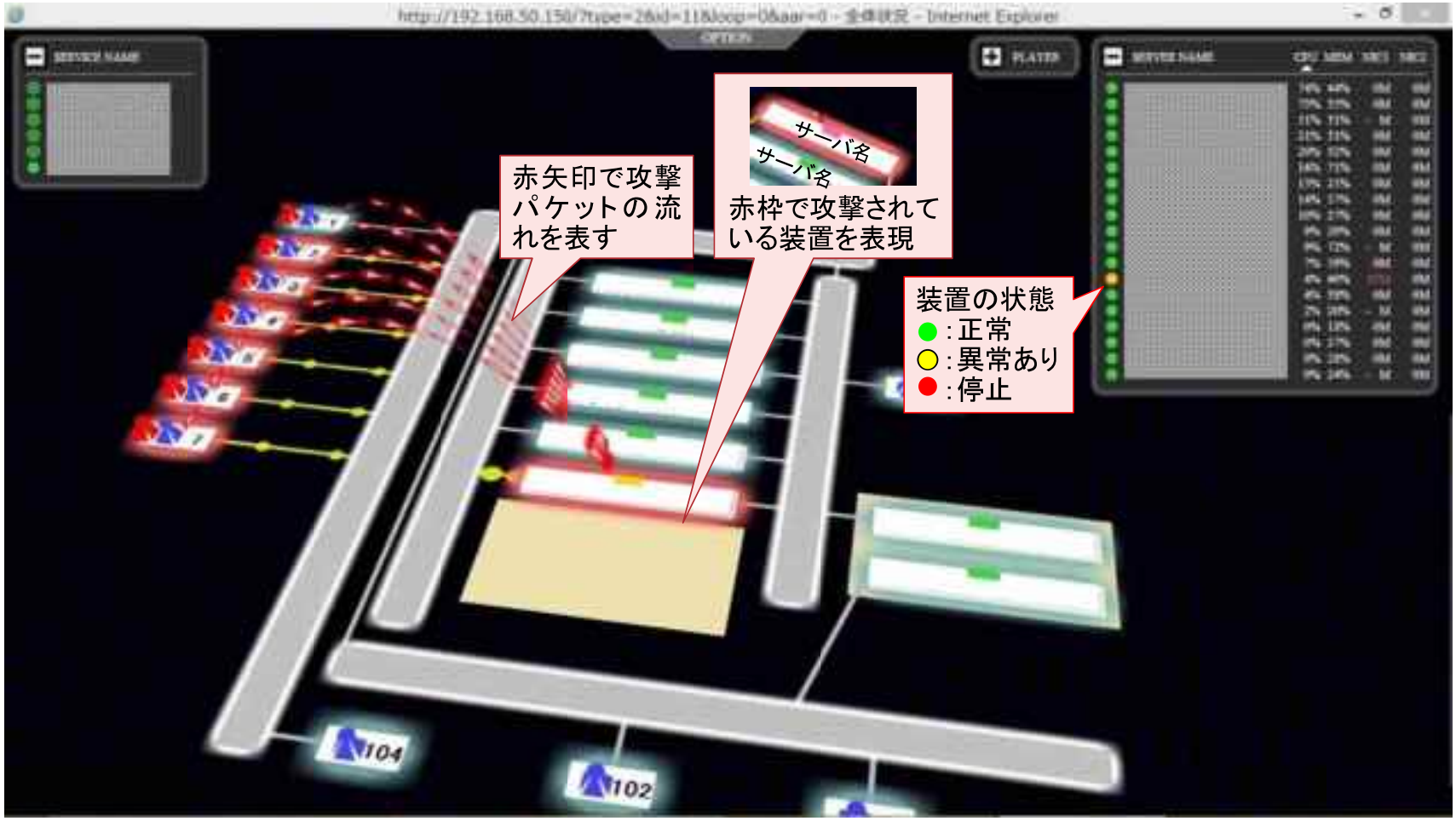


研究成果：サイバー演習環境構築技術（２/５）



マルウェアに感染した端末から他の端末へ感染が拡大する様子

研究成果：サイバー演習環境構築技術（３/５）



感染した端末からターゲットのサーバへ大量のパケットが送付されている様子

研究成果：サイバー演習環境構築技術（４/５）

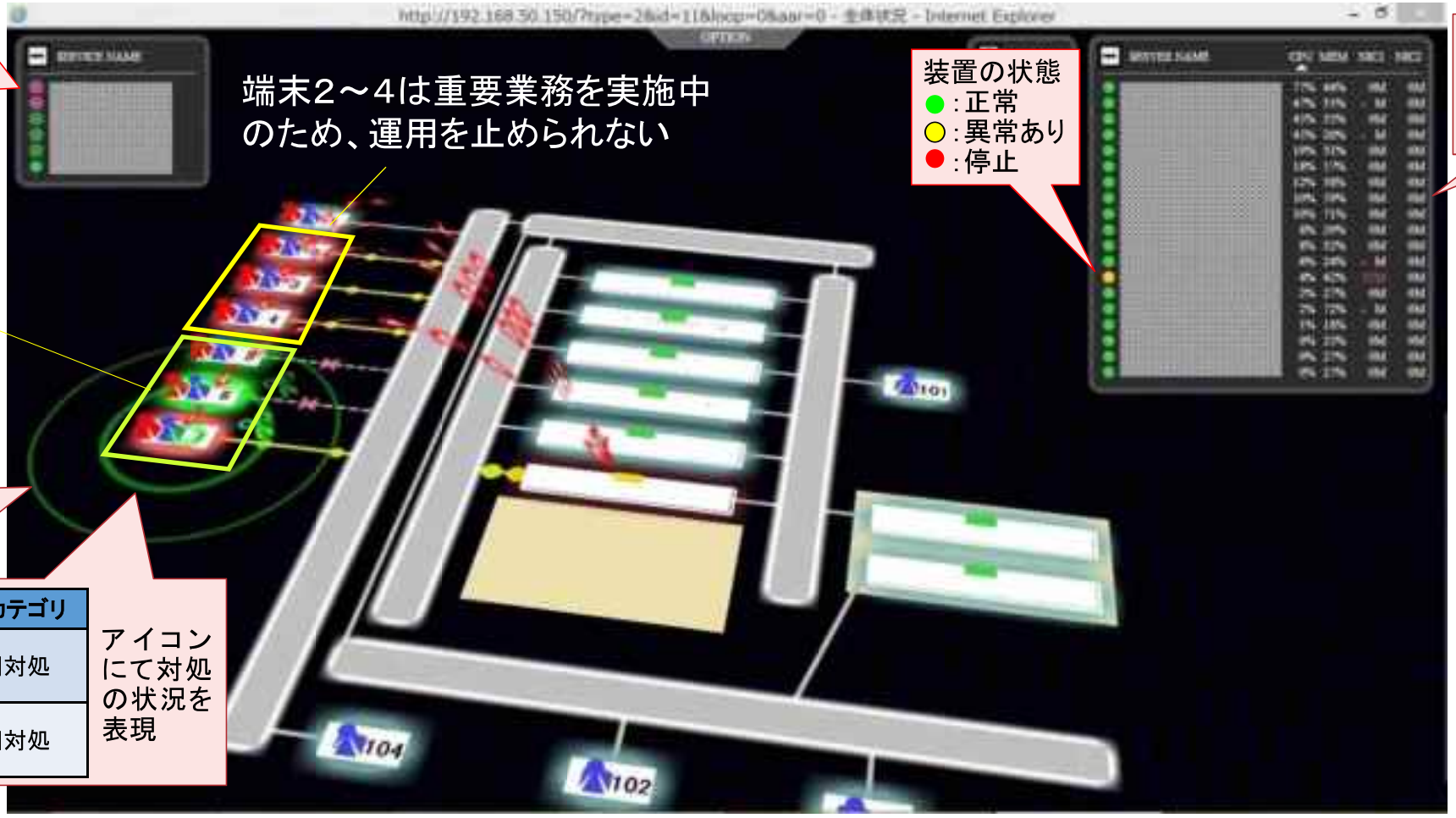
機能の状態
●:正常
●:異常あり
●:停止

端末５～７は運用を止めても問題ないと判断し、ネットワークから切り離し

波紋表示で対処操作が行われる予定の装置を表現

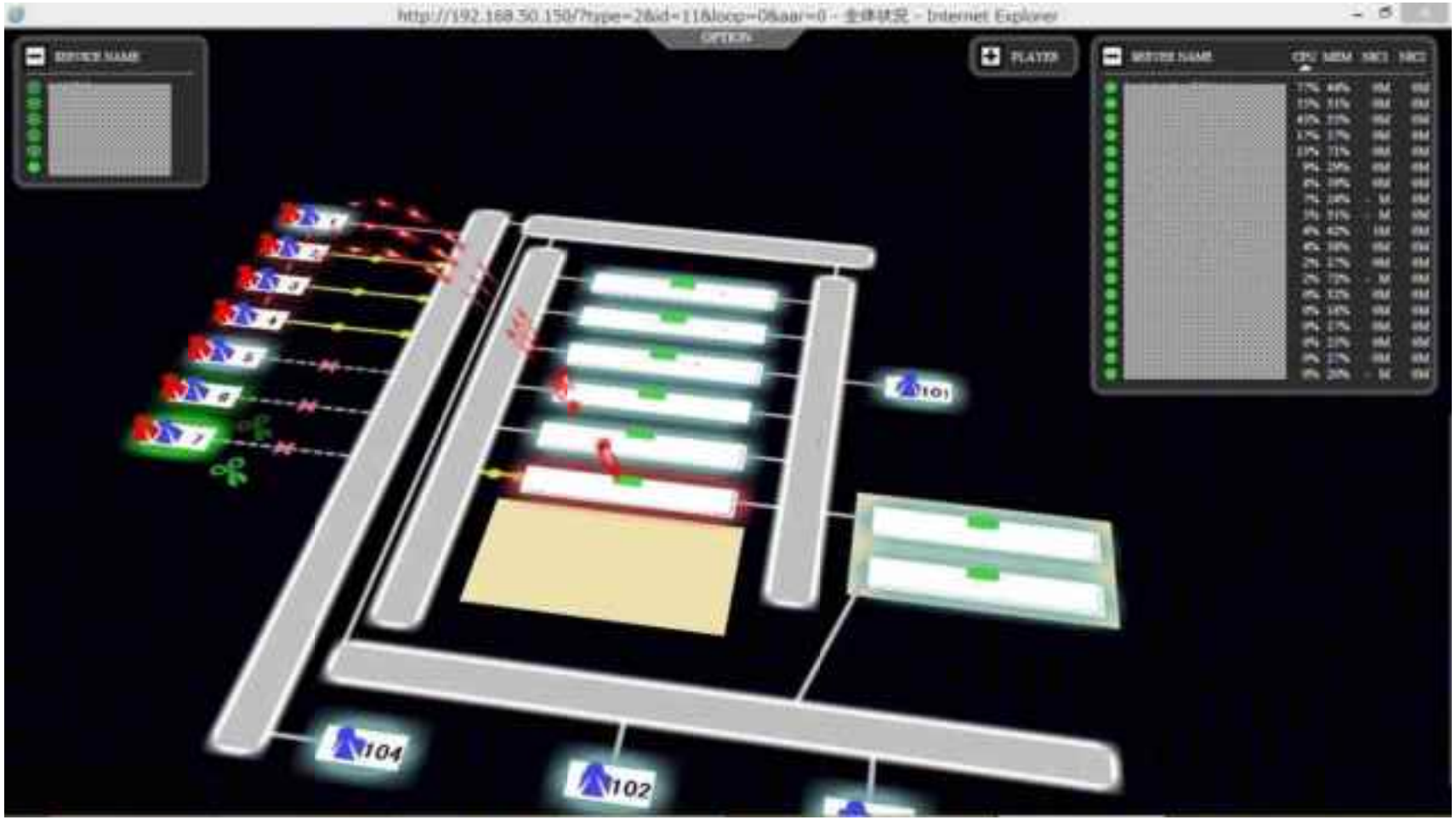
アイコン	対処カテゴリ
	初期対処
	原因対処

アイコンにて対処の状況を表現



システム管理者が攻撃元の端末をネットワークから切り離す措置をとっている様子

研究成果：サイバー演習環境構築技術（５/５）



攻撃による負荷が低減し、機能が回復した様子

今後の研究の方向性