防衛装備庁

サイバーセキュリティ技術の研究（1／2）

移動系サイバー演習環境構築技術の研究

研 究 背 景

防衛省・自衛隊のシステムは、様々なサイバー攻撃により効果的な指揮統制と情報共有が妨げられる危険にさらされています。サイバー攻撃による被害拡大防止と部隊運用継続を両立させ、システムの安定的な利用を維持するためには、サイバー演習環境が求められています。

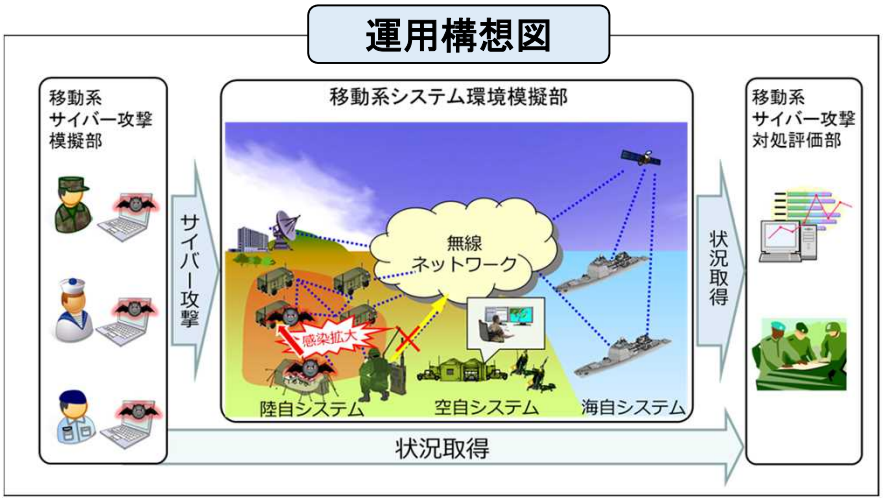
研 究 目 的

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の構築を目指した研究です。

研 究 内 容

- 移動系サイバー攻撃模擬
- 移動系サイバー演習統制情報収集
- 移動系サイバー演習環境復元

運用構想図



研究計画

年度	29（2017）	30（2018）	元（2019）	2（2020）	3（2021）	4（2022）
実施内容		研究試作			所内試験	

研 究 成 果

ネットワーク速度等に制約のある環境で、サイバー攻撃状況の再現、制御や情報収集等が可能とするよう設計いたしました。

防衛装備庁

サイバーセキュリティ技術の研究（2／2）

サイバーレジリエンス※技術の研究

研 究 背 景

防衛省・自衛隊においては、各種状況等に応じて重要システムの変更が発生し、また、複数拠点やネットワークがサイバー攻撃等の被害を受けた場合にも運用継続可能な制御を行う必要があり、このような状況に応じ迅速なシステム、ネットワークの制御が求められています。

※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

研 究 目 的

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ことを目指した研究です。

研 究 内 容

- サイバー攻撃の被害拡大防止
- 重要システムの運用継続
- 統制機能抗たん性確保

運用構想図

研究計画

年度	28（2016）	29（2017）	30（2018）	元（2019）	2（2020）	3（2021）
実施内容		研究試作 ←	→	所内試験 ←	→	

研 究 成 果

複数拠点にサイバー攻撃等の被害を受けた場合にも、運用継続を実現する制御を可能としました。