サイバー攻撃対処に関する研究

○加賀智也*、佐野裕香*、城間晴輝*、小森旭*、亀田健一*、坂下圭一*

1. 緒論

防衛省・自衛隊の保有するシステム及びネットワークは、平素から様々なサイバー攻撃の脅威を受けており、効果的な指揮統制及び情報共有が妨げられる危険に曝されている。それゆえ、指揮システムに対するサイバー攻撃等が発生した場合において、防衛省・自衛隊の作戦・指揮に必要なシステムの機能維持と、サイバー攻撃による被害拡大の防止を両立させることが求められている。

被害拡大防止と運用継続を両立させるためには、サイバー攻撃に対する「隊員の練度向上」と「任務遂行能力の確保」が必要となる。今回は上記を実現すべく実施中の2つの研究について報告する。

2. サイバーレンジ技術の研究

本研究は、指揮システムを模擬した実践的なシミュレーション環境でサイバー攻撃対処の訓練を行い、対処効果などについて評価を行い、サイバー攻撃対処の最適化と練度向上を図ることが可能なサイバー演習環境の構築に必要な技術を取得し、サイバー攻撃対処能力を強化するためのサイバー演習環境の構築に反映することが目的である。

サイバー演習環境を使用して訓練・演習を行い、サイバー攻撃対処の最適化と練度向上を図るためには、演習シナリオの質と作りやすさや演習環境が実際に業務で使用しているシステムと同等な環境であることが重要である。

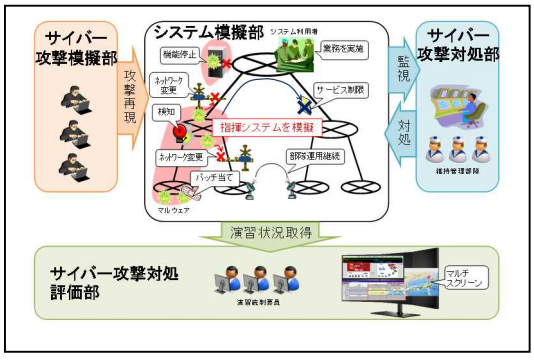

図１　サイバーレンジ技術の研究　運用構想図

本研究では指揮システムが使用される状況を想定したシナリオに対して、サイバー攻撃を状況付与することで、実戦的な演習シナリオを簡易に作成することが可能な方式を設計した。また演習で用いる模擬環境については、防衛省・自衛隊が実運用で使用している指揮システム等を模擬した環境を構築することで、より高い演習効果が得られる設計とした。

3. 動的セキュアネットワーク技術の研究

本研究はサイバー攻撃による被害があった場合でも「任務遂行能力の確保」を実現するための研究である。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両立するためのネットワーク統制技術を取得し、将来の防衛省・自衛隊のネットワークに反映することが目的である。

防衛省・自衛隊が用いるネットワークは各種事態に応じて動的に重要通信が変化するため、このような状況に応じ迅速なネットワーク制御ができることが重要である。

本研究では各種状況等の変化に応じて統制処理を行う方式及びサイバー攻撃等により統制機能に損失が発生した場合においても経路を維持する方式について現在設計を進めている。

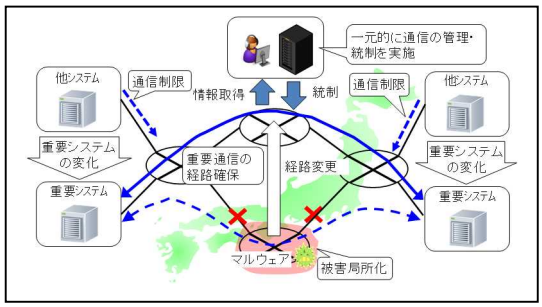

図２　動的セキュアネットワーク技術の研究　運用構想図

4. 今後の取り組み

今回報告する研究は現在、試作品の設計及び製品試験の段階であり、今後は性能確認試験を行い設計した手法等について検証を行っていく予定である。

*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