研究テーマ:不正アクセス等再現実験環境の統合手法に関する研究(1/2)

(プロジェクト番号　JGN2-A16054)

研究機関:　情報通信研究機構情報通信セキュリティ研究センター
北陸先端科学技術大学院大学

研究の概要:

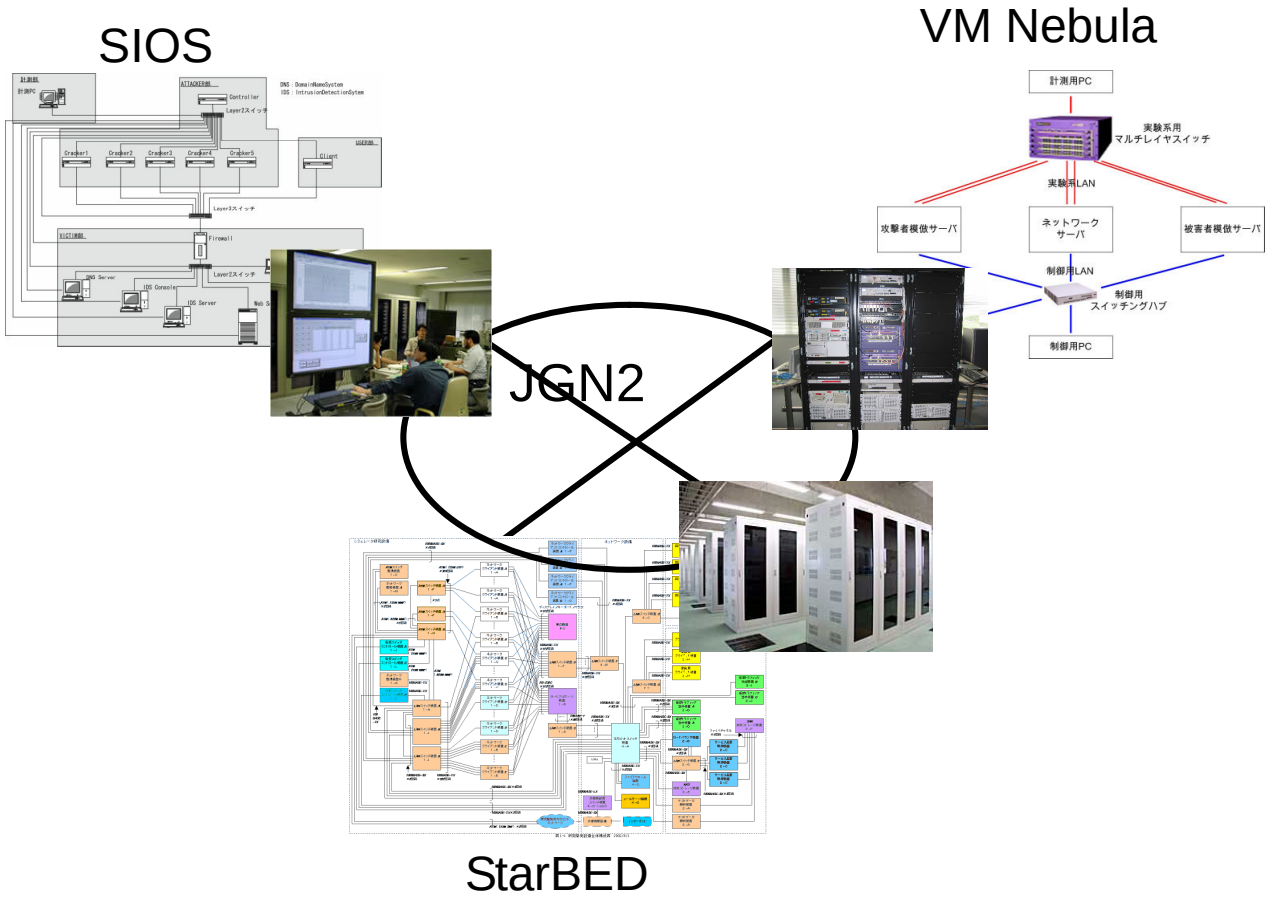
複数の異なる再現実験環境を統合することで、大規模かつ複雑な不正アクセス事案などの再現を可能とするための手法を確立する。統合手法を検討し、検証するために、我々が研究開発してきた3つの再現実験環境SIOS-StarBED-VM　NebulaをJGN2で相互接続し、実証実験を実施する。

研究の目的:

インターネット上での不正アクセスなどに対応するための、セキュリティ技術や対策手法の研究開発や検証には、実際のセキュリティ事案を再現・模倣して実験することができる再現実験環境が重要である。しかし、セキュリティ事案は年々大規模かつ複雑になってきており、一つの再現実験環境だけでは、規模や機能の面で不十分となってきている。

そこで、我々は今まで研究開発してきた再現実験環境同士をJGN2で接続し、相互に連携させることで、仮想的に実験環境の規模や機能の向上を図るため、不正アクセス等の再現実験環境の統合手法を研究開発する。

実験機器構成:



SIOS(NICT小金井本部)とStarBED(NICT北陸IT研究開発支援センター)を10Gbpsで、VM　Nebula(NICT関西先端研究センター)を1GbpsでJGN2を用いて相互接続している。

研究テーマ：不正アクセス等再現実験環境の統合手法に関する研究（2/2）

（プロジェクト番号　JGN2-A16054）

研究機関：　情報通信研究機構情報通信セキュリティ研究センター
北陸先端科学技術大学院大学

研究開発成果：

複数の実験環境の相互接続と連携・統合手法について、問題点を整理し、手法を検討し、統合手法について接続性能実験や実証実験を実施した。実験として、SIOS-StarBED-VM Nebulaの3つの再現実験環境をJGN2で物理接続し、再現実験を実施した。図1のようにそれぞれに再現ノードを配置し、DDoS攻撃の再現実験を実施した。

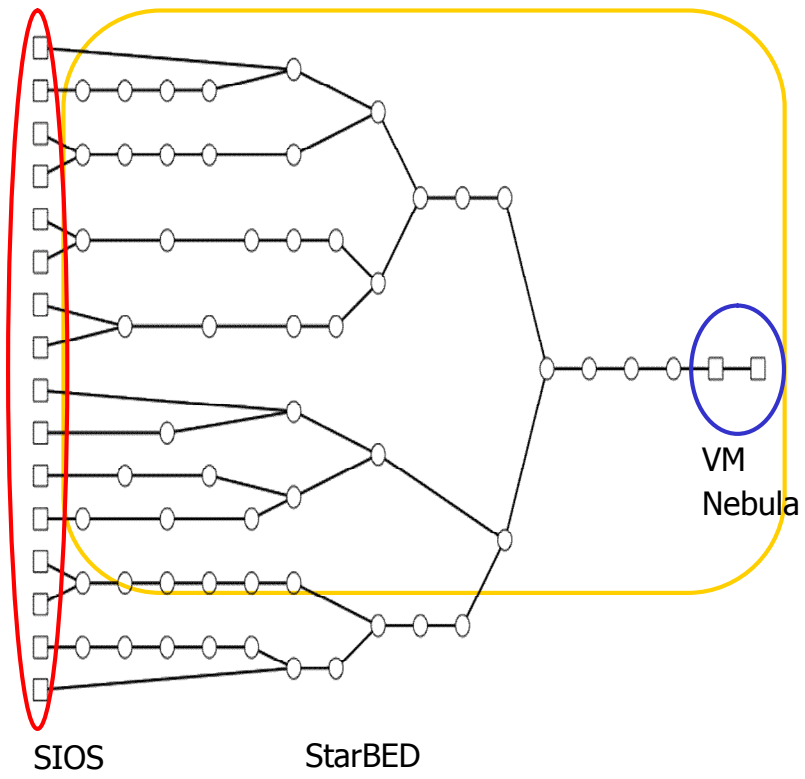


図 1. DDoS 再現実験

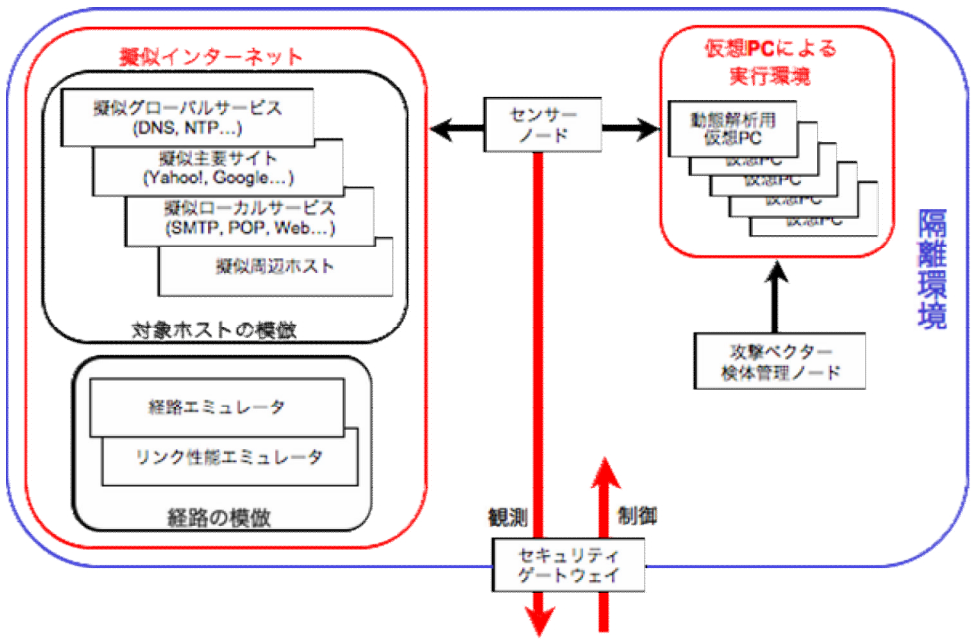


図 2. 擬似インターネット機能付きマルウェア解析環境

さらに、連携環境のリンクエミュレーション機能向上の検討や統合を指向した汎用アーキテクチャの提案を行った。これらの成果を利用した擬似インターネット機能付きのマルウェア解析環境（図2）を構築し、既存の解析環境では解析困難な事案の再現を可能とした。

プロジェクトのアピールポイント

この研究プロジェクトによって、複数の実験環境を接続する手法を一般化し、世界中に散在しているさまざまな実験環境が接続され、有効利用できるようになることが期待される。

プロジェクトの自己評価

実験環境間の接続に関する十分な手法検討と試行が実施できた。今後は今回利用したテストベッド以外と連携・統合するための手法の一般化や標準化などを行い、より広範な実験環境を連携・統合可能とする必要がある。