研究課題別事後評価結果

１．研究課題名：　サイバー脅威ビッグデータの解析によるリアルタイム攻撃検知と予測

２．研究代表者名及び主たる研究参加者名（研究機関名・職名は研究参加期間終了時点）

研究代表者

関谷　勇司（東京大学情報基盤センター　教授）

主たる共同研究者

島　慶一（(株) IIJ イノベーションインスティテュート技術研究所　副所長）

松浦　知史（東京工業大学学術国際情報センター　准教授）

門林　雄基（奈良先端科学技術大学院大学情報科学研究科　教授）

３．事後評価結果

○評点：

B　成果がやや不足している

○総合評価コメント：

サイバーセキュリティは CREST として取り組む価値の高い重要な社会課題であり，対策アシストを目標に据えて，その自動化とガイドラインを示すことを目標としたことは高く評価できる．

実データの大規模収集という難しい課題に取り組み，収集したデータセットの有用性を機械学習の適用により示し，インシデントの予測という極めて難しい課題を方向転換して現実的なインシデントレスポンス対策支援を目指した基礎検討が進んだ．一方で，異常挙動発見に画像認識や自然言語処理の既存手法を超える新規性を示すことも望まれた．

サイバーセキュリティの現場ではノウハウや暗黙知が必要で，論文化や新しい要素技術の訴求が難しい．また組織を横断してそれらを網羅性のある形式知とする研究の困難さがある．それを理解した上で，イスラエルなどサイバーセキュリティ分野に強みを持つ海外の機関と連携し，国際的なプロジェクトを組織するなどの展開を今後期待したい．

この研究は，セキュリティと人工知能の境界領域に属する研究であり，新産業を創出するほどの成果を生み出すチャンスはある．