先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	サイバーレジリエンス構成学 (門林　雄基　(教授))		
学籍番号	2111178	提出日	令和 5年 1月 18日
学生氏名	中川　桃李		
論文題目	MITRE ATT&CKを用いたフォレンジック適正向上を目的としたログ選定手法に関する研究		

要旨

昨今のサイバー攻撃の高度化により、従来行われてきた侵入を防ぐための入口対策では攻撃を防ぐことは困難な状況となっており、侵入を前提とした対策の必要性が高まっている. 侵入を前提とした対策では攻撃によって発生したログをフォレンジックすることで攻撃の全容を明らかにすることが重要となる.

この際、フォレンジックに必要なログが取得されていない場合はフォレンジックを行うことができず、またログが膨大に取得されている場合はフォレンジックに必要なコストが増加するため、どのようなログを取得するかによってフォレンジックの能力とフォレンジックを行うためのコストとの間にトレードオフの関係が発生する.

そのため、取得するログを事前に選定することでこれらのトレードオフを考慮し、組織ごとに適したログのみを取得することが必要となる.

既存のログ選定手法はガイドラインとの整合を目的としているため、取得するログとフォレンジック可能となる脅威との対応が明確化されていない.そのためログを取得することによるフォレンジックの効果を算出することは困難であり、効果とコストのトレードオフを考慮したログ選定は実現されていない.

これらの課題を解決するためには、フォレンジックを行う能力の最大化とフォレンジックに必要なコストの最小化を目的とするForensic Readiness(以降フォレンジック適正と呼ぶ)をログ選定において実現することが求められる.フォレンジック適正についてはフレームワークやフォレンジックの効率化などの手法が提案されているが、ログ選定に着目したものは存在しない.

そこで、本研究ではMITRE ATT&CKを用いて脅威シナリオから必要なログを抽出し、ログに対してフォレンジックにおける効果とコストを算出することで、対象となる脅威の明確化による効果の算出と効果とコストのトレードオフを考慮したログ選定手法の提案を行う.

評価として、複数の脅威シナリオに対するログの選定を行い効果とコストのトレードオフが明示化されることを確認し、提案手法がログ選定において有効であることを示した.