様式第 6 号

令和 2 年度実績報告書

令和 3 年 3 月 20 日

公立千歳科学技術大学
学長　川瀬　正明　様

公立千歳科学技術大学特別研究等助成要綱第 7 条に基づき、下記のとおり報告いたします。

報告者	所属	理工学部	職名	助教
	氏名	砂原 悟	ふりがな	すなはら　さとる
研究課題名	標的型攻撃における攻撃兆候の推論とインシデントレスポンスの高速化			
本研究費による発表論文、著書など	次年度以降に予定			

研究成果報告

[1] 研究の背景及び目的

昨今、出口対策と呼ばれるシグネチャベースのセキュリティ製品では検知できないような標的型攻撃を受けることがあり、被害の検知までに日数を要することが問題となっている。

本研究では、組織内におけるインシデントレスポンスを高速化する手法の開発を目的として、基幹システム 1 年分のログ収集し、攻撃として疑わしい通信の継続性、通信元、狙われやすい機材の有無を調査する。不正な通信および活動であると認められた場合にはラテラルムーブメントの可視化を行う。また、その通信、活動のログの特徴抽出を行い、機械的な学習データを生成する。

[2] 本研究によって得られた成果

効率的に分析を行うために重要となるログの集約を自動的に行うことができるようになった。また、図 1 のように通信のアクティビティの可視化を行うことで、管理者がこれまで見つけることができなかった組織内の不審な活動を見つけることができるようになった。本取り組みによって、不審なアクティビティが 3 件発見された。うち 1 件は実際にインシデントレスポンスが開始されており、実用性を確認することができた。図 1 の①については他のノードとは異なる形をしているため、見つけ次第確認するべき通信である。②についてもグラフの枝の先が正常な形と異なる、特徴的な形である。本取り組みでは、通信のほかにホスト内の疑わしい活動についても監視を行い、相互に比較することで、ゼロデイ攻撃や Windows Server のゴールデンチケット取得されるような攻撃についても検知が可能である。図 2 はホスト内で発生した疑わしい活動(PowerShell を用いた模擬的な攻撃)を可視化したグラフである。組織の管理者は通信の状況を相互に確認することによりラテラルムーブメントを確認することが可能となった。図 3 は疑わしい活動の期間(継続性)を可視化したグラフである。期間のスケールは 5 分～365 日までを選択できる。

[3]課題について

本研究では、[2]で得られた成果を機械的に検出する手法を開発することで、インシデントレスポンス開始までの時間を短縮することを目的としていたが、データ可視化の作業にて遅れが発生し、ログから特徴抽出及び機械的な学習データの生成には至っていない。ホスト内のアクティビティを可視化するための Sysmon Search と Elastic Search(オープンソースソフトウェア)の構築がうまくいかず、急遽 Graphviz による実装に変更したことが遅れの要因となった。データとしては実用的であることが確認できているため、引き続き機械化の作業を行い、次年度以降に論文発表を行う予定である。

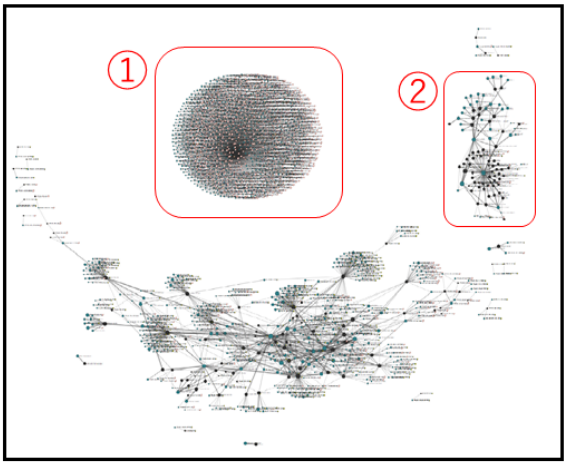

図 1 通信のアクティビティを可視化

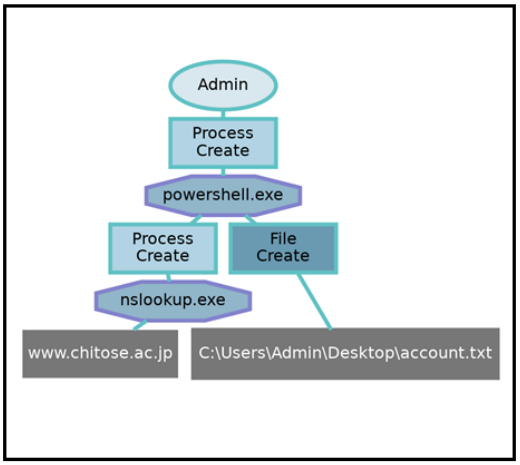

図 2 ホスト内のアクティビティを可視化

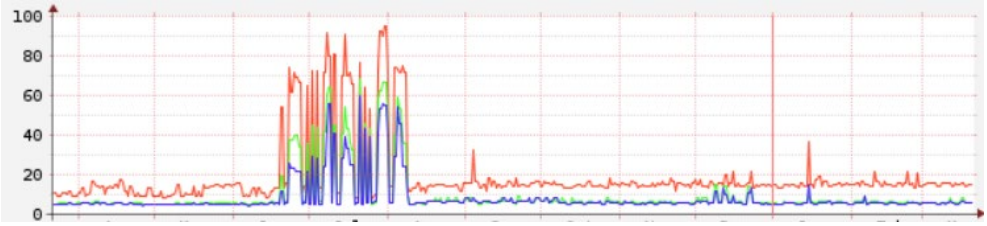

図 3 疑わしい活動の期間を可視化