効果的なサイバー攻撃の脅威情報分類の検討
Study of effective Cyber Threat Classification

天野 純一郎・情報セキュリティ大学院大学

Abstract: Recently cyberattacks against private companies and government organizations to steal information such as PII(personally identifiable information), IP(intellectual property), authentication credentials and others has become a serious problem. One reason for this may be the fact that underground market has been formed and monetization method has been completed. Additionally, many kinds of attacks become easier to carry out. Because of these, threat actors now have both motivations and methods in hand. However, on the defenders side, who has been targeted by these actors, have to pay increasing costs. To protect these targeted defenders effectively the organizations need to recognize cyber threats and go through cyber risk assessment process. These risks can be resolved into threats and vulnerabilities. Previous researches on risk information are focused on classificating those. On responding to individual query such as statistical graph for executives are created by human. In this papers, issues and assumptions on gathering and combining threat information is discussed.

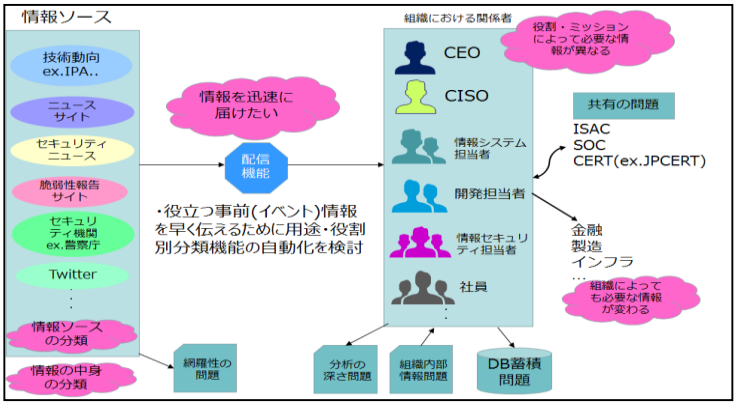
はじめに

近年，企業や組織に対する，情報窃盗などを目的としたサイバー攻撃が深刻な問題となっている．サイバー攻撃を行う攻撃主体は，インターネットから攻撃ツールを容易に入手できたり，サイバー空間の地下市場により利益を得ることができるため，被害組織と比べ常に優位に立ち続けている．

孫子は兵法の中で，「If you know the enemy and know yourself, you need not fear the result of a hundred battles.；彼（敵）を知り，己を知れば百戦してあやうからず．」と述べている．被害組織は，サイバー攻撃の脅威情報を入手して，敵と己を知ることが重要である．つまり組織は，各組織ごとにサイバー攻撃の脅威情報を入手・活用する手段が必要である．

本稿では，資源の有効活用を目指し，日々大量に公開されるサイバー攻撃に関する脅威情報について，敵と自分を素早く知ることにつながる脅威情報の効果的な分類および配信を検討する．

研究のスコープ



まとめ

本稿では，サイバー攻撃に関する脅威情報を組織が有効活用するために，情報を利用する者に着目して分類を検討した．

先行・関連研究

Edwin Tump氏は，先行研究の中で，情報配信をタイムリーに行うことを目的として，CERT組織の情報収集・配信を一元化するフレームワーク Taranisの提案・構築を行っている．このTaranisにより，異なる情報源や，異なるツールを利用したアウトプット作成など，複雑なオペレーション体系が改善された[1].

また，Edwin Tump氏は，Taranisで収集した情報に関する新たな課題について研究を行っている．この研究では，収集される情報量が，1日に約6,000件と大量なため，これらの情報を高速に処理するために，機械学習のアプローチを用いて，既に収集している事象との関連性を明らかにし，情報配信をタイムリーにすることを目指している[2].

提案手法

さらに迅速に情報を届けるために，組織における関係者は異なる役割やミッションにより必要となる情報が異なるだろうと仮定し，まだ検討されていない，配信のための分類機能の自動化の提案を行う．

これが実現されることにより，関係者に対して迅速に情報を届け，組織におけるサイバー攻撃に対する耐性やリジリエンスを高められる可能性がある．

各組織における関係者が必要とする情報を洗い出し，情報の配信部分における自動分類手法について，着目し実装方法について検討する．

具体的には，以下の3つが実装可能性について検討を行う予定である．

①組織における関係者が必要とする情報の種類を洗い出しクラスタリングを行い的確な情報配信が行えるかどうか検討を行う．

②広告配信などでは，マーケティングを目的として消費者に対して的確な広告を表示するように取り組んでいる，この手法を役割ベースの情報配信に利用できないか検討を行う．

[1]Edwin Tump. Taranis: turning your sources into reusable security alerts. NISHA Workshop in Zurich. <入手先 http://www.nisha-network.eu/sites/default/files/20140212-NISHA-workshop-Taranis.pdf> (2016/01/16 アクセス)
[2]Edwin Tump. Machine Learning for Cyber Security Intelligence. 27th FIRST Conference. <入手先 https://www.first.org/resources/papers/conf2015/first_2015_-_tump-_edwin_-_machine_learning_for_cyber_security_intelligence_20150611_fw.pdf> (2016/01/16 アクセス)