プレッシャーによるサイバー攻撃兆候検知に向けた検討

Study on Detecting Indications of Cyber-Attacks using Pressure.

石井友基・マネジメント分科会・情報セキュリティ大学院大学

Abstract ：
Threat of Cyber-Attacks is expanding from Cyberspace to Real space by propulsion of IoT. It need to take measures of Cyber-Attacks at an early stage because it is assumed situation which Cyber-Attacks is directly linked to human life. It is thought to detect that indicate of Cyber-Attacks using "PRESSURE" about motive of attacker. The analysis reveals the possibility to detect indication of attack for evaluations of pressure on a trial basis using cases of past attacks.

研究のサマリ

目的：攻撃の予防や被害の極小化に資すること

◆攻撃兆候に対するプレッシャー活用の検討
◆過去の攻撃事例を用いてプレッシャーを評価
◆プレッシャー評価の実装に向けた予備検討

攻撃兆候を「プレッシャー」として表現するモデルを示した

日々大量に発生しているアラートについて
対処の優先順位付けができると考える

プレッシャーに着目

動機の獲得を把握できれば
攻撃兆候といえるのではないか

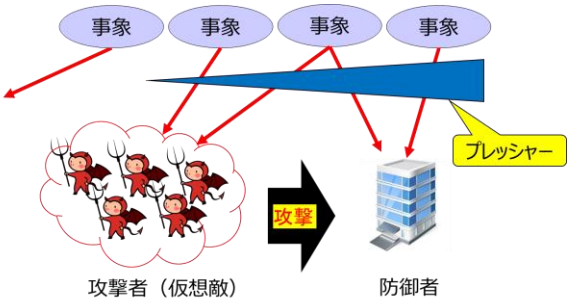
攻撃者は、行動を起こす前に、原因・理由・背景など
攻撃を行うための動機を獲得すると想定

しかし

動機は非常に複雑な要因が絡んでおり、個々人の内面、
心理的側面に関わってくるため、直接的に把握することは難しい

そこで

動機を獲得することに影響すると考えられる様々な事象を
プレッシャーという指標で単純化して表す



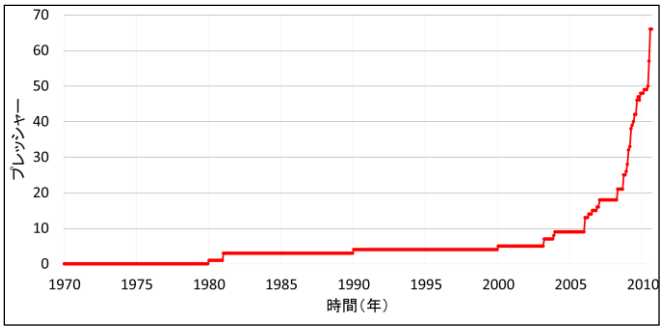
プレッシャーの評価手順

①定義	自組織に対する脅威と攻撃者（仮想敵）を想定し、プレッシャーを増減させるような事象を定義する
②収集	①で定義した想定脅威に基づき、③で分析を行うために必要な情報を収集する
③分析	①で定義したプレッシャーを増減させる事象を，②で収集した情報から抽出してスコアリングする
④評価	③でスコアリングした結果を，ある単位ごとに集計し可視化した上で最終的にプレッシャーを評価する

過去事例を用いたプレッシャー評価

◆Stuxnet事例
2010年に核開発阻止のため米国とイスラエルがイランの核関連施設をサイバー攻撃したとされる事例

◆用いたスコアとプレッシャーを増減させる事象例
＋１：非難声明、議決、採択
＋２：リアル攻撃高まる（サイバー攻撃を選択してリアル攻撃を回避）
＋３：サイバー作戦計画、継続判断、脆弱性公表
－１：査察容認、核燃料生産停止を示唆
－２：IAEAの査察実施、リアル攻撃しないことを示唆
－３：脆弱性修正、サイバー攻撃計画中断
（－２、－３の事象は確認できなかった）



◆10年以上前からプレッシャーが徐々に高まっていた
◆直前5年間はプレッシャーが急激に増加していた

プレッシャーによって攻撃兆候を把握できる可能性

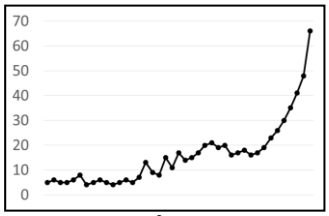
プレッシャーの活用想定

【想定①】対処開始の判断

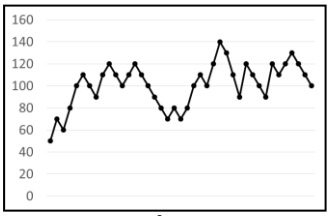
ポートスキャンが発生
＋
プレッシャーが増加している
↓
対処開始

【想定②】優先順位の判断

A社とB社で同時にアラート発生
＋
A社とB社のプレッシャーを相対的比較
↓
A社を優先して対処



A社のプレッシャー



B社のプレッシャー