5W-08

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

石井　友基†　　後藤　厚宏†

情報セキュリティ大学院大学†

1. はじめに

サイバー攻撃は年々と高度化・巧妙化しており，情報漏えい事件を中心にサイバー攻撃の被害は後を絶たない．さらに，IoT（Internet of Things）が推進される中，サイバー攻撃による大規模停電や自動車に対する脅威事例など，サイバー空間から実空間へ脅威が広がりつつあり，サイバー攻撃が人命に直結する事態も想定されることからも，より早い段階で攻撃対策を行う必要がある．

標的型攻撃の流行以降は，従来の入口対策から，侵入されることを前提とした内部対策および出口対策にシフトしてきた．しかし，それらの対策は，米国ロッキード・マーティン社が提唱しているサイバーキルチェーンにおける第 3 段階「デリバリ」以降を対象としており，現状では第 2 段階以前の対策が充分とは言えない．

そこで，攻撃の予防や被害の極小化のために，より早い段階で攻撃対策を行うことを目的として第 2 段階以前に着目し，「プレッシャー」という指標を用いて攻撃の兆候を掴むことを検討する．

2. 攻撃兆候活用の現状

第 1，第 2 段階において兆候と考えられる事象の例を表 1 に示す．

表 1．兆候と考えられる事象の例

段階	1	2
	偵察	武器化
事象（例）	●ポートスキャン（攻撃のため，マルウェア作成のため） ●攻撃対象を検索，ソーシャルエンジニアリング	●マルウェア購入のための資金集め ●マルウェア売買のためのダークウェブ徘徊 ●マルウェアの作成，試行

第 1 段階「偵察」で発生したポートスキャンを例に考えると，どのような状況下でポートスキャンを検知した場合に攻撃の兆候と言えるのか，それだけで兆候と判断し警戒態勢をとれるのか，といったことを明確に定義できるだけの知見が現状はない．この事象を兆候と言うためには，例えば，第 3 段階「デリバリ」で受信した標的型メールの送信元と第 1 段階「偵察」のポートスキャンの送信元が同一であったというパターンが考えられる．しかし，このパターンでは第 3 段階まで攻撃が進行していることになり，ポートスキャンを検知したという事象を攻撃兆候として有効活用できているとは言えない．

McAfee 脅威レポート［1]によると，インシデント対応組織の 1 つである SOC（Security Operation Center）の運用状況について，地域，業界，企業規模の異なる 400 人のセキュリティ専門家を対象に調査した結果として以下を挙げている．

●93%の組織が脅威の優先度を判断できていない
●膨大なアラートのうち調査できているのは 25%
●回答者のうち 3/4 は，未調査のアラートがビジネスに影響を及ぼしていると回答

上記より，防御側はリソースが足りていないため，攻撃が始まっている第 3 段階以降を優先したインシデント対応を行っていると考えられる．その状況下において，前述の例に挙げたポートスキャンのような第 1，第 2 段階で発生する「兆候かもしれないが兆候とは定義できない怪しい事象」に対して，防御側が脅威を評価して適切な対応判断を行うことは難しい．そして，多くの事例を積み重ねてポートスキャンを攻撃兆候であると定義するために，コストを投入することも困難である．

したがって，何らかの新たな判断材料を示し，「怪しい事象」を有効活用できるようにする必要がある．

3. プレッシャーによる兆候検知へのアプローチ

最初に，攻撃の兆候とする期間を設定する．どの段階を攻撃発生とするかについては，侵入を試みた時点，侵入された時点，目的が達成された時点など様々な観点が考えられるが，本稿では第 3 段階を攻撃発生とし，第 3 段階以降を攻撃期間，第 2 段階以前を兆候期間とする．

そして，「攻撃活動を始める前に，攻撃者は何らかの原因・理由・背景によって攻撃を計画する動機を獲得している」と想定し，キルチェーンに第－1 段階として「動機の獲得」を設定する（図 1）．

図 1．本稿におけるサイバーキルチェーン

動機の考え方の一例として，平成 22 年度犯罪白書[2]で挙げられている殺人の動機を以下に示す．

「憤まん・激情」「報復・怨恨」「痴情・異性関係トラブル」「利欲目的」「暴力団の勢力争い等」「検挙逃れ・口封じ」「介護・養育疲れ」「心中企図」「虐待・折かん」「被害者の暴力等に対抗」「その他」

上記のように，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，攻撃者が抱える動機を直接的に把握することは難しい．

そこで，攻撃者の内面にあって通常は表すことができない動機の代わりに，攻撃者が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ことを検討している．最初に，どのような脅威が存在するかを想定し，プレッシャーを増減させる社会系事象やサイバー系事象（表 2）を定義する．

Study on Detecting Indications of Cyber-Attacks using Pressure.
†Yuki ISHII，Atsuhiro GOTO.
†INSTITUTE of INFORMATION SECURITY.

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

次に，SNS や Web などインターネット上で収集したデータから定義した事象を抽出する．最後に，抽出した各事象を単純な数値でスコアリングし，積算することでプレッシャーの動向を把握する．

表 2．プレッシャーを増減させる事象の例

プレッシャー	社会系事象	サイバー系事象
高める	経済・情勢悪化，事件・テロの発生，会談拒否，非難声明，核開発推進，思想信条に反する事象，自由侵害，不正・汚職発覚，職場環境悪化，競合他社が新製品発表	新脆弱性公開，攻撃ツールの公開，マルウェアトラフィック増，脆弱性放置，設定ミス，ポリシー違反，過剰な情報公開，他組織におけるサイバー攻撃
下げる	首脳会談，擁護・支持，査察受け入れ，謝罪，環境改善	パッチ公開，マルウェア対策強化，脆弱性対応，設定修正

4. プレッシャーの試験的評価

過去の攻撃事例から，2010 年にイランの核関連施設を狙って行われたとされる Stuxnet 事例について，試験的に以下のスコアを用いてプレッシャー評価を行った．

●スコア
＋1：非難声明，議決，採択
＋2：リアル軍事攻撃高まる
＋3：サイバー作戦計画，継続判断，脆弱性公表
－1：査察容認，緊張緩和，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」については，実空間における軍事攻撃による中東情勢悪化を回避することを目的に Stuxnet 攻撃が計画された背景があるとされていることから，リアル攻撃の可能性が高まるほどサイバー攻撃の実行に踏み切る可能性が高まることを想定している．なお，「－2」，「－3」の事象については確認できなかった．Stuxnet におけるプレッシャーのスコアリング結果を図 2 に示す．

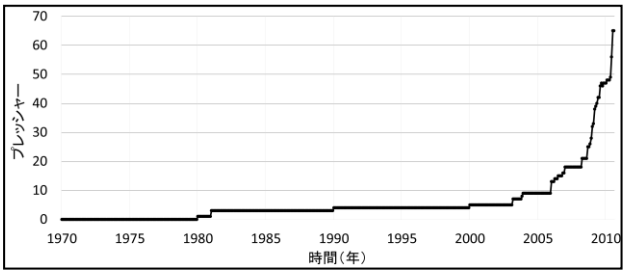

図 2．Stuxnet 事例を用いたプレッシャー評価例

図 2 から，「10 年以上前からプレッシャーが徐々に高まりつつあり，最終的な攻撃が行われるまでの約 5 年の間はプレッシャーが急激に増加している」といったことをプレッシャーによって把握できる可能性を示している．当時，事前にこの可能性を兆候として掴むことができていた場合，攻撃を防ぐための何らかの対策を年単位の余裕をもって実施できたのではないかと考える．

5. プレッシャーの活用想定

SOC において以下の状況が発生したと想定する．

●ポートスキャンを検知した
●過去の検知事例では攻撃に至っていない

この状況下において，SOC 担当者が「攻撃の兆候かもしれない」という可能性を認識していたとしても，2 章で述べたように，他にも調査すべきアラートは膨大にあること，過去の検知事例では攻撃に至っていないことから，攻撃とは言えない状況に対して何らかの調査や対応を継続するためにコスト投入を判断することは難しい．

そこで，仮に図 2 のようにプレッシャーが急増していることが判明していた場合，SOC 担当者は「ポートスキャンは兆候であり，攻撃に発展する可能性がある」と判断して対応を継続することもできる．

対処すべきか否か迷った際はプレッシャーの値や変動，傾向を見たり，複数の事案が発生しどちらを優先すべきか迷った際はプレッシャーの大小を比較したりすることで，防御側の判断材料の 1 つとしてプレッシャーを活用できるのではないかと考えている．

6. 関連動向

JPCERT/CC などは，インターネット全体の健全性とリスクを各国／地域ごとに算出し比較可能な指標（cyber health）で可視化することで，各国の CSIRT や ISP などとデータを共有・連携して健全なインターネットの実現を目指すサイバーグリーンプロジェクトという取り組みを行っている[3]．マルウェアトラフィック，ボットネット感染率，脆弱性，インシデント数，OS アップデートなどの情報を用いて評価している．

川北ら[4]は，攻撃対処に必要な情報収集を効率化することを目的に，金融工学領域で用いられるテクニカル分析の活用を検討している．具体的には，ソーシャルメディアにおける脆弱性やマルウェアに関する投稿の数がピークに達する兆候を掴み，関連するサイバー攻撃の発生を早期に予測することを目指している．

どちらも，第 3 段階以降を含むサイバー系事象を対象としており，社会系事象は評価対象となっていない．

7. まとめと今後の課題

攻撃兆候検知に向けて，第 1，第 2 段階において発生した怪しい事象に対する防御側の判断材料の 1 つとするために，第－1 段階で発生した事象をプレッシャーとして評価する方法を示した．

今後は，プレッシャーを活用するための一連の流れを「定義」「収集」「分析」「評価」のフェーズに落とし込み，システム化するために必要な検討事項をフェーズごとに整理していきたい．そして，プロトタイプの実装や評価を行い，さらに具体的な検討課題を抽出したい．

参考文献

［1］McAfee,『McAfee 脅威レポート：2016 年第 3 四半期』, 2016 年 12 月
［2］法務省,『平成 22 年版 犯罪白書 第 7 編/第 2 章/第 1 節/1』,2010 年 11 月
［3］『Cybergreen』, http://www.cybergreen.net/,（2016 年 11 月 27 日参照）
［4］川北ら,『テクニカル分析によるサイバーインシデント予測手法の検討』, 2016 年 3 月

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.